DIAGNÓSTICO DEL ESTADO Y NIVEL DE SEGURIDAD DE LA INFORMACIÓN VIGENTE EN LA EMPRESA DISEMEQ LTDA DEL DEPARTAMENTO DE CASANARE – DISEINFORDI.

JUÁN ANDRÉS USCÁTEGUI NIÑO
C.C: 4.104.861

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
YOPAL CASANARE
2014

DIAGNÓSTICO DEL ESTADO Y NIVEL DE SEGURIDAD DE LA INFORMACIÓN VIGENTE EN LA EMPRESA DISEMEQ LTDA DEL DEPARTAMENTO DE CASANARE - DISEINFORDI.

JUÁN ANDRÉS USCÁTEGUI NIÑO
C.C: 4.104.861

Trabajo Presentado como proyecto de grado

Ingeniera
EDNA ROCÍO BERNAL MONROY
Director de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
YOPAL CASANARE
2014

Preliminares

Nota de aceptación

_____
_____
_____
_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Preliminares

AGRADECIMIENTOS

Agradezco a Dios por guiarme, bendecirme con salud e inteligencia y permitirme concluir una etapa más en mi proceso de formación profesional; a mi madre María Magdalena niño quien fue la mujer elegida por Dios, para darme la vida, donde me guio, enseño a ser una gran persona y desde el cielo acompaña mis días, a mi padre Roberto Uscategui, quien ha sido mi ejemplo de vida donde reconforta mi moral y mi espíritu. A mis hermanos, Lilia, Clara, Estella, Floro, Luz marina, Angela, que son el pilar de mi familia. A mi amada esposa Patricia, quien ha sido el impulso durante toda mi carrera, que con su apoyo constante y amor incondicional para salir adelante, a nuestros hijos por motivarme cada día a superarme como persona y profesional. A mi directora, por guiarme en la estructuración de mi proyecto de grado; a mis profesores que compartieron sus conocimientos y dedicaron su tiempo para hacer posible este sueño. A la Universidad Nacional Abierta y a Distancia “UNAD” por brindarme las bases necesarias para definir mi perfil como profesional integral, con capacidades cognoscitivas e intelectuales para satisfacer las necesidades de la comunidad y contribuir con el progreso dinámico y el desarrollo tecnológico que demande la sociedad. A mis amigos, quiero agradecerles que de una u otra manera estuvieron pendientes a lo largo de este proceso, brindado todo su apoyo incondicional que se tomaron la molestia de gastar un poco de su tiempo para explicarme las cosas que no entendía, Hoy en día los amigos son algo muy raro y escaso le agradezco a Dios por mandarme unos amigos honestos y sinceros que no buscan nada a cambio, solo buscan ayudar a los demás para poder superarse en la vida, hago una dedicación muy especial de este proyecto a mi padre que sido la persona más ejemplar del mundo y que gracias a él he surgido como persona.

Preliminares

TABLA DE CONTENIDO

Preliminares

Preliminares

LISTA DE IMÁGENES

Preliminares

Preliminares

LISTA DE TABLAS

Cuerpo del proyecto

INTRODUCCIÓN

Este proyecto pretende diagnosticar el estado y nivel de seguridad de información vigente en la empresa Disemeq Ltda ubicada en la ciudad de Yopal en el Departamento de Casanare, esta empresa se dedica a prestar los servicios explotación y desarrollo de la Ingeniería Mecánica, Civil. Para promocionar y comercializar, sus servicios lo hace a través de un sitio web llamado http://disemeqltda.com/, y correos electrónicos.

La empresa Disemeq Ltda, tiene una red de 22 computadores conectados mediante una red cableada y otros por conexión Wifi, la infraestructura de red tiene unas características de seguridad muy básicas lo que hace que su información y sus equipos están siendo vulnerables a los ataques informáticos, como la infección de virus troyanos, gusanos, malware, que han atacado los sistemas que en ésta empresa se manejan. Los riesgos a los que se ven expuestas las empresas hacen necesario la creación de directrices que orienten hacia un uso responsable de los recursos. Las políticas de seguridad son documentos que constituyen la base del entorno de seguridad de una empresa y deben definir las responsabilidades, los requisitos de seguridad, las funciones, y las normas a seguir por los empleados de la empresa “Según un estudio realizado recientemente, 8 de cada 10 equipos se encuentran infectados con algún tipo de código malicioso. Ante estos datos tan alarmantes, la Microsoft ha elaborado una Guía de Seguridad que intenta describir los pasos prioritarios que una empresa debe implementar para proteger su entorno. Es necesario enfatizar en la necesidad de un cambio de concepción, que conlleva al empleo de medidas proactivas en la gestión de la seguridad. Las medidas reactivas son soluciones parciales, medidas de protección implementadas sin apenas intervención del

usuario, que básicamente consisten en “la instalación del producto” sin un seguimiento y control continuo”[1]. Ressio N. (2009).

Este diagnóstico tuvo como objetivo primordial tomar la información recopilada sobre el estado actual, las falencias, amenazas, revisión física del hardware también del software, se hizo el análisis de la infraestructura de toda la red, como cableado, equipos de conexión, portátiles, estaciones de trabajo, también se realizó una encuesta a varios funcionarios para recoger información valiosa que nos sirviera de base para atacar de raíz el problema, y por último el estado de la seguridad informática.

La empresa Disemeq Ltda nunca se había preocupado por la seguridad de su infraestructura de red y la información que maneja internamente; debido a que la red no tiene mucha seguridad, por no tener un firewall que filtre el acceso y un antivirus licenciado que ayude a proteger; hace un tiempo comenzó a sufrir de ataques a su red; tales como: virus informáticos troyanos, spam, malware, accesos sin autorización al sistema operativo, daños al hardware: tales como quemado de memorias RAM, Main Board, Procesador. Por esta razón se realizó el diagnóstico para obtener un informe o documento, que sirviera de guía, soporte y orientara las directrices consolidadas con el fin de determinar las soluciones que permitan mejorar la seguridad de toda la red y la protección de toda la información de la organización. También se entregó un manual de las políticas de seguridad informática, lineamientos y uso de equipos dentro de la organización; en el diagnóstico irá la simulación de un software especializado en redes (Packet Tracer) para demostrar cómo se encontraba la infraestructura antes y como se debe implementar de según las normas, para evitar problemas de seguridad en la empresa Disemeq Ltda.

[1] http://www.elmundodelastics.net/2009/07/9-pasospara-implementar-la-seguridad.html#.U-QXA-N5NsM

Cuerpo del proyecto

El objetivo principal de este diagnóstico es analizar el estado actual de la infraestructura de red y el nivel de seguridad informática existente en la empresa Disemeq Ltda, con la recopilación de esta información buscar las posibles soluciones a las que debe realizar una implementación en la empresa para mejorar su seguridad informática y protegerla contra diversos ataques que son la debilidad más grande que tienen la mayoría de las empresas en el mundo.

Por otra parte, este proyecto se realiza para optar al título de especialista en seguridad informática en la Universidad Nacional Abierta y A Distancia “UNAD”, y se pretende implementar en la empresa Disemeq Ltda para mejorar la seguridad y así acabar con todos los problemas de seguridad informática en esta organización.

Cuerpo del proyecto

1. TEMA

Realizar un diagnóstico del estado y nivel de seguridad de la información vigente en la empresa Disemeq Ltda del Departamento de Casanare, el proyecto "Diagnóstico del estado y nivel de seguridad de la información vigente en la empresa Disemeq Ltda del Departamento de Casanare – DISEINFORDI. se encuentra enfocado hacia la línea de Infraestructura Tecnológica y Seguridad en Redes (Cadena Ingeniería Electrónica, Telecomunicaciones y Redes).

2. PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

En la actualidad las empresas privadas han experimentado transformación en algunos aspectos de seguridad; la situación actual permite comprobar que los sistemas informáticos son el activo más valioso y al mismo tiempo el más vulnerable. La seguridad informática ha adquirido gran auge, dada las cambiantes condiciones y nuevas plataformas de computación disponibles, situación que converge en la aparición de nuevas amenazas en los sistemas informáticos.

Generalmente encontramos que no se invierte en el capital humano y económico necesario para prevenir el daño y/o pérdida de la información confidencial en las empresas, lo que genera muchos problemas relacionados con el uso de computadoras, amenazas que afectan negativamente tanto a individuos como a

empresas; la proliferación de la computadora como la principal herramienta, así como la creación de la red global Internet ha provocado que cada vez más personas se las ingenien para lucrarse, hacer daño o causar perjuicios.

"El auge de la tecnología y las telecomunicaciones en la actualidad ha permitido tener el acceso fácilmente a cualquier tipo de información; en Latinoamérica durante el 2012, el 50% de las empresas han sufrido ataques informáticos muy frecuentes durante todo el año, siendo la mayor preocupación en materia de la seguridad de la información[2]" Mundofranquicia, (2010). haciendo que los sistemas informáticos sean susceptibles de ataques de virus, accesos no autorizados entre otros, que pueden afectar los sistemas en general; estos son los motivos por los que se hace necesario implementar estrategias de seguridad y protección de bases y redes de información de diferentes empresas y entidades estatales, como es el caso de Disemeq Ltda. Ubicada en Yopal Casanare, donde vemos que la parte de redes especialmente la infraestructura tecnológica está mal diseñada y que la seguridad en el acceso a las estaciones de trabajo son muy débiles e ineficientes, por tal razón nos corresponde hacer un análisis para determinar el estado de la seguridad informática en esta entidad privada y mejorar para estar preparada para los avances al siglo XXI.

2.2 DEFINICIÓN DEL PROBLEMA

Disemeq Ltda, ha solicitado continuamente profesionales que solucionen problemas ocasionados con daños en el hardware y software, causado por continuos ataques y proliferación de virus, malware, perdida de información, pero aunque solucionan de momento no han llegado al fondo del asunto, ya que el problema principal que tiene la empresa, es que cuando implementaron la red no tuvieron en cuenta los requisitos mínimos para brindarle protección, fueron

[2] http://www.mundofranquicia.com/reportaje.php?num=520

adecuando más computadores pero no implementaron un firewall que les filtrara toda la navegabilidad y los contenidos; su información creció desprotegida y por ende es vulnerable a sufrir cambios inesperados.

2.3 FORMULACIÓN DEL PROBLEMA

¿Qué necesita la empresa DISEMEQ LTDA, para mejorar su nivel de seguridad informática?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un diagnóstico para analizar el estado actual de la infraestructura de red y el nivel de seguridad informática existente en la empresa Disemeq Ltda. Con el fin proteger los recursos informáticos valiosos de la organización, tales como la información el hardware o el software.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar una caracterización en el nivel de seguridad informática de la empresa Disemeq Ltda.
- Analizar la infraestructura tecnológica (Hardware-Software) y redes de telecomunicaciones existentes en la empresa Disemeq Ltda.
- Evaluar el estado en que se encuentra la seguridad de la información en la empresa Disemeq Ltda.
- Generar un manual de las políticas de seguridad informática, lineamientos y uso de equipos dentro de la organización.
- Realizar una simulación con un software especializado en redes (Packet Tracer) sobre toda la infraestructura de red de Disemeq Ltda.

Cuerpo del proyecto

- Generar un documento que presente las soluciones que permitan aumentar y mejorar el nivel de seguridad de la información en Disemeq Ltda.

Cuerpo del proyecto

4. MISIÓN EL PROYECTO

Realizar un diagnóstico del estado y nivel de seguridad de la información vigente en la empresa Disemeq Ltda, del Departamento de Casanare, que sirva de base para buscar las falencias, debilidades y las posibles soluciones que mejoren su seguridad informática.

5. VISIÓN DEL PROYECTO

Buscar y mejorar, la calidad de la infraestructura de red, el nivel de seguridad de la empresa Disemeq Ltda, y promover seguridad informática para los diversos ataques informáticos, que continuamente están sufriendo las empresas ocasionados por los delincuentes informáticos.

6. JUSTIFICACIÓN

La seguridad informática, de igual forma como sucede con la seguridad aplicada a otros entornos, trata de minimizar los riesgos asociados al acceso y utilización de determinados sistemas no autorizados y en general malintencionada.

Los sistemas de información en la actualidad están siendo constantemente afectados por diferentes tipos de acciones maliciosas que ponen en riesgo la seguridad informática, siendo un nuevo motivo de preocupación para diversos entes y organismos, debido a los incidentes de seguridad que se han presentado en diferentes organizaciones, conduciéndolas a tomar conciencia de su importancia. Esta visión de la seguridad informática implica la necesidad de gestión, fundamentalmente gestión de riesgo; para ello, se deben evaluar y

cuantificar los bienes a proteger, y en función de estos análisis, implantar medidas preventivas y correctivas que eliminen los riesgos asociados o que los reduzcan hasta niveles manejables. Teniendo en cuenta lo mencionado anteriormente, se hace necesario desarrollar, tomar e implementar medidas o planes de seguridad que permitan eliminar posibles riesgos potenciales. Por esto se quiere generar un informe completo sobre el estado y el nivel de la seguridad de la información vigente en la empresa Disemeq Ltda, para saber en qué condiciones se encuentra y cuáles son las posibles falencias de seguridad informática que presenta esta organización, con el fin de dar soluciones concretas, que reduzcan y permitan fortalecer las políticas de seguridad de esta entidad. Hoy en día, tener un sistema que cumpla con los estándares de gestión de la seguridad es sinónimo de calidad de servicio.

Este proyecto “Diagnóstico del estado y nivel de seguridad de la información vigente en la empresa Disemeq Ltda del Departamento de Casanare – DISEINFORDI”. Se realizó para optar al título de Especialista en Seguridad Informática de la Universidad Abierta y a Distancia UNAD de la Escuela de ciencias Básicas Tecnología e Ingeniería y se hizo para suplir una necesidad vista en la empresa Disemeq Ltda, donde tiene problema de seguridad informática, donde se realizó la socialización del proyecto a Disemeq Ltda, y a ellos les gustó la idea por lo que nos dieron una carta de aceptación para realizar este proyecto en dicha empresa.

En este diagnóstico se realizará un análisis de las vulnerabilidades del hardware y del software, el cual pretende garantizar que el estado y uso de la información que se maneja en la empresa Disemeq Ltda, sea una fuente segura, confiable y confidencial a la cual solo tenga acceso el personal autorizado. Además establecer políticas de seguridad dentro de la organización para mitigar todos los riesgos posibles de seguridad informática en esta empresa.

Cuerpo del proyecto

7. MARCOS DE REFERENCIA

7.1 MARCO TEÓRICO

La empresa Disemeq Ltda, se encuentra ubicada en la ciudad de Yopal en la Cra. 24 No. 33 – 60 tiene un edificio de dos (2) pisos donde en el primer piso se encuentra la parte administrativa y el segundo piso están los empleados que se encargan de toda la elaboración de los procesos licitatorios, en la parte de atrás del edificio se encuentra la bodega y el almacén donde almacenan los equipos y la herramienta con la que trabajan en diferentes ciudades del Departamento de Casanare. Actualmente está compuesta a nivel de su infraestructura con una red doméstica de 22 computadores conectados por una red cableada de 8 equipos conectados por medio de un Switch marca Trendnet de 32 puertos distribuidos por cable UTP de nivel 4, por todo el edificio construido hace aproximadamente 10 años, por lo que es mucho tiempo de estar instalados estos cables ya que la vida útil del cable UTP es de aproximadamente 5 años. Por otra parte tenemos una red inalámbrica (WIFI) de 14 computadores portátiles, los cuales se encuentran conectados mediante un router inalámbrico marca Trendnet de 4 puertos de capacidad de 80 metros de alcance, la capacidad de ancho de banda es 2 megabyte por segundo en rehusó, suministrada por el operador ISP Movistar, la mayoría de los equipos de conexión están incrustados en un gabinete de 65cmx40cmx40cm en metal, ubicados debajo de la escalera en un cuarto muy estrecho con poca ventilación, sin aire acondicionado, expuestos al polvo, también se guardan los elementos de aseo de la empresa, lo cual es inadecuado porque lleva humedad a todos los equipos. También posee un circuito cerrado de televisión con 8 cámaras marca walcon para la seguridad física del edificio. Hay que aclarar que la forma como están conectados los computadores actualmente mediante el Switch marca Trendnet no es la correcta, ya que debe estar antes de este Switch un equipo firewall que haga filtrado de contenido y filtrado de acceso

con el fin de evitar intrusos y accesos malintencionados, por tal razón se dice que tiene una red doméstica porque los computadores están conectados pero no se ha implementado ninguna seguridad según como lo indica la norma para su correcta protección.

En cuanto al software que se maneja dentro de la empresa Disemeq Ltda, los portátiles y en los computadores de escritorio todos tienen Windows 7 y 8 solo tienen licenciamiento 8 de los 22, y el software aplicativo no tiene licenciamiento como es el paquete office (Word, Excel, powerpoint, access), el autocad, lo cual es nocivo para la empresa por no acatar lo dispuesto en LEY 603 DE 2000, por la cual se modifica el artículo 47 de la Ley 222 de 1995, sobre software ilegal en Colombia.

Por otra parte los computadores no tienen un antivirus licenciado ya que poseen antivirus gratis (AVAST, AVG) lo cual protege pero muy básico y no es igual como si fuera un antivirus que cubra todos los protocolos de seguridad como las diferentes formas de ataques a los equipos.

Otro software que se manejan en Disemeq está el **SIESA 8.5** es un software contable y lo manejan por conexión de acceso remoto pero este está muy bien protegido ya que es distribuido por la empresa en diferentes ciudades y esta albergado en un servidor con todos los protocolos de seguridad. También se maneja el correo electrónico de Microsoft Outlook que cumple con todos los lineamientos de seguridad porque está albergado en un servidor seguro y cada usuario posee su contraseña de seguridad para acceder al correo ya sea por página web o por el software Outlook del paquete Office.

Cuerpo del proyecto

7.1.1 INFORMACIÓN GENERAL DE LA EMPRESA DISEMEQ LTDA

Empresa	:	DISEMEQ LTDA.
TIPO DE ENTIDAD	:	SERVICIOS DE INGENIERÍA
Dirección	:	Cra. 24 No. 33 - 60 Yopal Casanare
Teléfax	:	6357411
Nit	:	844002122-1

7.1.2 BREVE RESEÑA HISTÓRICA

La empresa Disemeq Ltda, fue fundada en el año 2000, por Ramón Octavio Moreno Plazas, en una sociedad de tipo limitada dedicada a la explotación y desarrollo de la Ingeniería Mecánica y Civil. En sus inicios sus actividades estuvieron representadas en el desarrollo de obras menores relacionadas con el objeto social. En la actualidad, se proyecta hacia la construcción y montaje total de líneas de flujo, como gasoductos, oleoductos y obras eléctricas, de instrumentación civiles en general. Comercializa sus servicios a través de un sitio web llamado http://disemeqltda.com/ correos electrónicos, presenta propuesta a otras empresas especialmente petroleras, se encuentra ubicada en la ciudad de Yopal posee un edificio de dos pisos, donde se encuentra estructurada en una red de 8 computadores conectados por cable UTP y 14 portátiles conectados mediante conexión Wifi. Su información es manejada y almacenada en los computadores de cada usuario, también poseen un software propio llamado SIESA con el que trabajan la parte contable de la empresa por conexión remota, el correo electrónico de Microsoft Outlook acceden a un servidor se encuentra

alojado en la ciudad de Bogotá y cada usuario posee su contraseña de seguridad para acceder al correo ya sea por página web o por el software Outlook.

7.1.2 MISIÓN

Basados en las exigencias técnicas de la ingeniería y en los compromisos con la calidad, en DISEMEQ LTDA se realizó obras mecánicas, eléctricas, civiles, y de instrumentación en el conexionado de pozos, construcción de líneas, mantenimiento de líneas y estaciones para el fluido de hidrocarburos, atendiendo los requerimientos del cliente de una manera oportuna y eficaz[3] (Disemeq Ltda. 2011).

7.1.3. VISIÓN

Para el año 2014 DISEMEQ LTDA, será un sólido proveedor ofreciendo para sus clientes en el sector hidrocarburos credibilidad en el desarrollo de sus proyectos, adoptando los mejores estándares normativos, legales y administrativos, desarrollando relaciones mutuamente beneficiosas con todas las partes interesadas[4] (Disemeq Ltda. 2011).

7.1.4. SERVICIOS QUE OFRECE DISEMEQ LTDA

Los servicios que a continuación se relacionan son ofrecidos a través de un sitio web llamado http://disemeqltda.com/ correos electrónicos, donde presenta sus propuesta a otras empresas especialmente petroleras, y participa en licitaciones

[3] http://www.disemeqltda.com/nosotros.php

[4] http://www.disemeqltda.com/nosotros.php

ofrecidas por portales web y para comercializar sus productos utiliza un grupo de profesionales capacitados ubicados en Disemeq Ltda y por ende los 22 computadores lo emplean para presentar sus ofertas al público. Los servicios que ofrecen son:

Trabajos en campo.

- "Construcción de oleoductos y gaseoductos bajo Código API.
- Reparación en oleoductos, gaseoductos y acueductos
- Montaje de equipos en Estaciones de Producción e interconexión mediante tuberías.
- Prefabricación y montaje de tanques atmosféricos y a presión, bajo códigos ASME y API
- Prefabricación y montaje de estructuras
- Construcción de bases para equipos, hangares de compresores y bombas, etc.

Trabajos en taller.

- Prefabricación de tanques atmosféricos y a presión.
- Fabricación de Estructuras.

Obras civiles.

- Mantenimiento de vías.
- Alcantarillados.
- Locaciones para perforación de pozos petroleros"[5] (Disemeq Ltda. 2011).

[5] http://www.disemeqltda.com/nosotros.php

Cuerpo del proyecto

7.1.5. LOGO DE DISEMEQ

Logotipo de identificación de la Empresa Disemeq Ltda.

Ilustración 1 Logo de Disemeq Ltda**.**

7.1.6 ORGANIGRAMA DISEMEQ

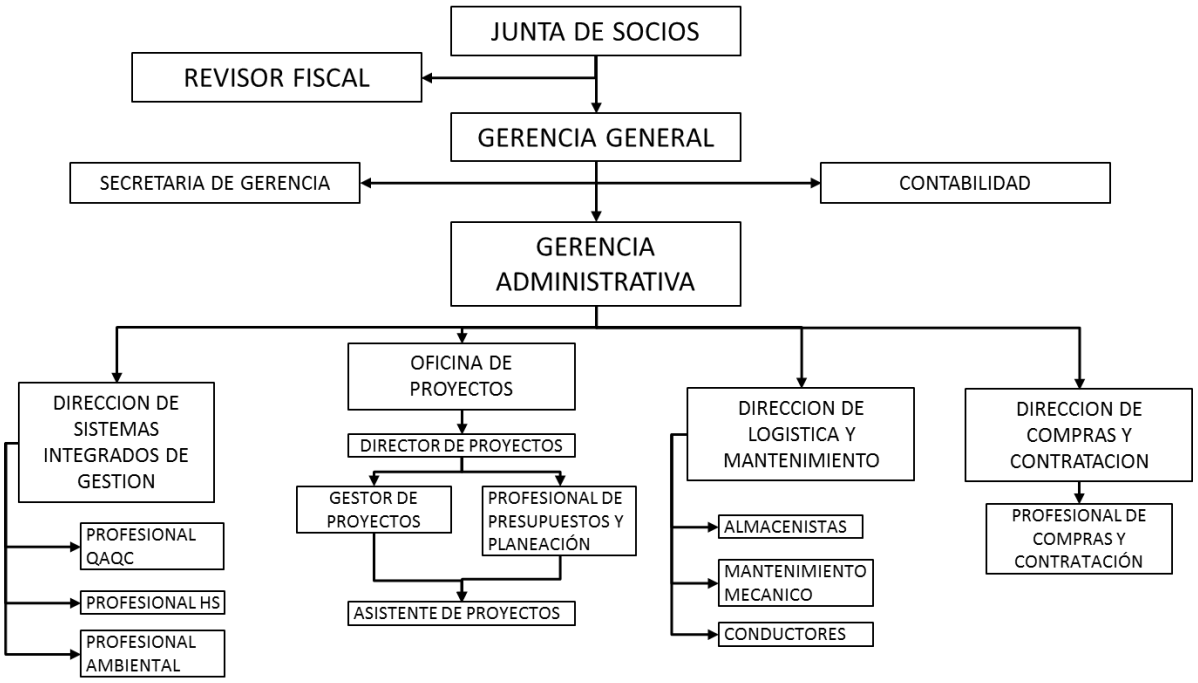


Ilustración 2. *DISEMEQ Ltda,* (2011). *Organigrama Disemeq Ltd.* Recuperado de http://disemeqltda.com/index.php

7.2 MARCO CONCEPTUAL

Cuerpo del proyecto

El proyecto “Diagnóstico del estado y nivel de seguridad de la información vigente en la empresa Disemeq ltda, del Departamento de Casanare – DISEINFORDI. Nos enfoca a diagnosticar el problema de seguridad informática en una empresa llamada DISEMEQ LTDA, y se necesita unos términos que constituyen el problema objeto de estudio como es la detección de necesidades para la implementación de la solución del problema.

Podemos llegar a creer que tanta seguridad en nuestro entorno informático termina por convertirse en algo molesto, pero lo cierto es que nunca viene mal tener una forma extra de protección. El internet por ser una red de redes está lleno de información útil, como también de virus navegando y buscando donde infectar y hacer daño a los usuarios que navegan por ella, al punto de volverse muy sofisticados en sus métodos, y de paso causar una buena dosis de paranoia. Por tal razón es necesario colocar un firewall adicional para sumar protección de seguridad informática, su instalación es cuestión de un par de minutos.

En Disemeq Ltda, se encuentra instalada una red doméstica con 22 computadores se llama domestica porque no posee ninguna protección de seguridad informática, ya que como lo hemos dicho no posee un firewall para filtrar acceso y contenido no dispone de un antivirus que proteja la red y su información por lo que debemos segmentar la red, de la siguiente manera: Los computadores que están conectados por cable se deben conectar por medio de una dirección IP que identifique cada uno de ellos en la red con el nombre del cargo que tiene cada usuario y los computadores portátiles también se debe colocar una dirección IP nombrados de la misma forma. Por lo que la red cableada estaría plenamente identificada, separada de la red inalámbrica. Y el acceso a la información interna será restringida para evitar robos y manipulaciones malintencionadas. En resumen queremos disponer que la solución al problema de seguridad informática en Disemeq Ltda, la damos en la fase siete (7) donde después de hacer una análisis a toda la red damos las soluciones que deben implementarse para acabar de raíz

con la inseguridad informática que actualmente está sufriendo. A continuación damos unos conceptos que son fundamentales a tener en cuenta en la seguridad.

Seguridad Informática: Es el "área de la informática que se enfoca en la protección de la infraestructura tecnológica y todo lo relacionado con ésta, incluyendo la información obtenida. Luego, su finalidad es asegurar que los recursos del sistema de información de una organización sean empleados de forma correcta, de acuerdo a las políticas establecidas, y que el acceso a la información, así como su modificación, sólo le sea permitida a las personas capacitadas y autorizadas. Con el fin de reducir los riesgos dentro de una organización, se tienen en cuenta una serie de estándares, leyes y protocolos, los cuales hacen de la Seguridad Informática una disciplina, encargada de diseñar una serie de procedimientos y técnicas, obteniendo un sistema de información seguro y confiable"[6] Mejia N. (2013).

Firewall: Es un dispositivo que tiene software o hardware que le da seguridad a una red, filtrando sistema que controla el tráfico de red entrante y saliente basado en conjunto de reglas y dando preferencias de administración. Muchas computadoras personales sistemas operativos incluyen firewall basados en software para proteger contra las amenazas de la Internet pública.

Red Plana: Es una red doméstica sin seguridad para poder compartir carpetas, archivos y conexión a Internet entre todos los equipos del hogar. Ya sea su conexión por cable o inalámbrica.

Red Segmentada: Es una red bien organizada, que ofrece mucha seguridad y pretende evitar la difusión de software malintencionado en la red de una empresa,

[6] http://blog.smartekh.com/seguridad-informatica-proteccion-desde-el-principio/

puede utilizar firewall para dividir la red de la empresa o LAN en segmentos y crear una arquitectura de red segmentada. Cada segmento puede administrar el tráfico de red para un componente específico. Y tiene implementación de direcciones IP fijas para su conectividad donde permite la comunicación entre varios dispositivos al mismo tiempo. El establecimiento de una conexión permite que los dispositivos compartan información, como archivos personales, e Internet.

Amenazas en Seguridad Informática: El usuario que consciente o inconscientemente causa un problema de seguridad informática. Programas maliciosos como virus, troyanos, programas espía, botnets, etc. Un intruso que consigue acceder a los datos o programas a los cuales no tiene acceso permitido. Un incidente, como una inundación, un incendio o un robo que provocan la pérdida de equipos o información.

Actores que amenazan la seguridad: Los principales actores de una red son; los hackers, cracker, lamer, copyhacker, bucanero, phreaker, newbie, script kiddie, tonto o descuidado, los ex empleados.

Tipos de Amenaza:

AMENAZAS LÓGICAS: Intencionadas virus malware uso de herramientas acceso no autorizado software incorrecto provienen de errores cometidos de forma involuntaria por programas.

AMENAZAS FÍSICAS: Fallos en los dispositivo catástrofes naturales terremotos.

8. TIPO DE INVESTIGACIÓN

De acuerdo al proyecto propuesto, se va a enfocar a una investigación mixta, donde vamos a tener en cuenta el enfoque cuantitativo porque se va a cuantificar una red de computadores y equipos que la componen y un enfoque cualitativo porque se va a cualificar el estado de la infraestructura de red actual y el estado y nivel de seguridad informática en esta misma red.

9. DELIMITACIÓN DEL PROBLEMA

Disemeq Ltda, carece de un diagnóstico o caracterización completo que nos arroje el estado actual de la infraestructura de red, y el nivel de seguridad informática de la red de computadores que actualmente se maneja, por tal razón es necesario realizar este estudio donde arroje la base para comparar las características técnicas reales de implementación de una red bien estructurada y buscar las falencias que se están teniendo con relación a la infraestructura de red y el estado y nivel de seguridad informática en esta empresa.

Este proyecto “Diagnóstico del estado y nivel de seguridad de la información vigente en la empresa Disemeq Ltda del Departamento de Casanare – DISEINFORDI. Fue necesariamente hacerlo, porque la empresa Disemeq Ltda, ha tenido varios ataques informáticos, tales como virus informáticos; troyanos, spam, malware, accesos sin autorización al sistema operativo, daños al hardware: tales como quemado de memorias RAM, Main Board, Procesador. Por esta razón se realizó el diagnóstico para obtener un informe o documento, que sirviera de guía, soporte y nos orientara a directrices consolidadas con el fin de determinar las

soluciones que permitan mejorar la seguridad de toda la red y la protección de toda la información de la organización.

10. TEMÁTICA

Disemeq Ltda, normalmente ha tenidos continuas pérdidas de información y ataques de virus, de malware, ocasionado por las fallas que se están teniendo. En este estudio se buscó las falencias, debilidades, soluciones de la empresa Disemeq, empezando con la revisión bibliográfica del tema, seguido de la encuesta, reconocimiento de las instalaciones, infraestructura y la revisión técnica, después se hizo un análisis de nivel y estado de seguridad, y por último la generación del informe o documento, el cual se sustentará y se pondrá en práctica para implementar las normas básicas de seguridad informática.

11. UNIVERSO

Este proyecto “Diagnóstico del estado y nivel de seguridad de la información vigente en la empresa Disemeq Ltda del Departamento de Casanare – DISEINFORDI. Va dirigido a las personas que hacen parte directa o indirectamente de Disemeq Ltda, como son los directivos, administrativos, empleados, clientes potenciales, amigos, todas las personas que conforman a Disemeq Ltda, ya que tienen que ver con la seguridad informática directa o indirectamente, para el mejor desarrollo de su trabajo, aplicaciones y así brindar un mejor servicio en todo sentido.

Cuerpo del proyecto

12. METODOLOGÍA

Este proyecto pretende hacer análisis de las vulnerabilidades, falencias, debilidades de Disemeq Ltda, en cuanto a la seguridad de la información, la cual comenzó por la caracterización de la infraestructura actual de la red implementada, luego la determinación de las amenazas e impactos sobre la infraestructura de la red, seguido por el análisis de la vulnerabilidad y determinación de la calidad de los controles o servicios de seguridad con la gestión de los riesgos, luego se entrega un manual (medio magnético) de las políticas de seguridad informática, lineamientos y uso de equipos dentro de la empresa para que implemente una capacitación y ponerlo en práctica con los empleados por último entregamos las diversas soluciones que permitan aumentar y mejorar el nivel de seguridad de la infraestructura de red y la seguridad de la información en Disemeq Ltda.

ANÁLISIS DE ENCUESTA

Se realizó una encuesta a 10 empleados de la empresa Disemeq Ltda, para encontrar las fallas de seguridad informática más comunes, y el manejo que se le da a la información dentro de la organización y las políticas de seguridad que se establecen en la empresa. Por tal razón el análisis queda así:

Cuerpo del proyecto

PROYECTO: DIAGNOSTICO DEL ESTADO Y NIVEL DE SEGURIDAD DE LA INFORMACIÓN VIGENTE EN LA EMPRESA DISEMEQ LTDA DEL DEPARTAMENTO DE CASANARE			
NUMERO	**PREGUNTA**	**RESPUESTA**	**CANTIDAD**
1	¿Cuáles son las fallas más comunes de su computador en Disemeq?	A. Problemas de antivirus o licencias	2
		B. lento el equipo y problemas de software	2
		C. ninguna	1
2	Cómo archiva u organiza la información de su computador en Disemeq Ltda?	A. En carpetas y archivos	2
		B. En CD, Discos duros, Memoria USB	2
		C. ninguna	1
3	¿Sabe usted si Disemeq Ltda, tiene políticas de seguridad informática para proteger la información?	A. SI	0
		B. NO	5
		C. No sabe	0
4	¿Qué tipo de seguridad implementa para proteger su computador?.	A. Por medio de contraseñas	2
		B. coloca contraseña a los archivos del computador	1
		C. ninguna	2
5	¿visita usted con frecuencia las redes sociales dentro de Disemeq para buscar alguna información?.	A. SI	2
		B. NO	3

Tabla 1. *Uscategui J.* (2014). *Análisis General* ***de la encuesta*** Recuperado el 24 septiembre de 2014

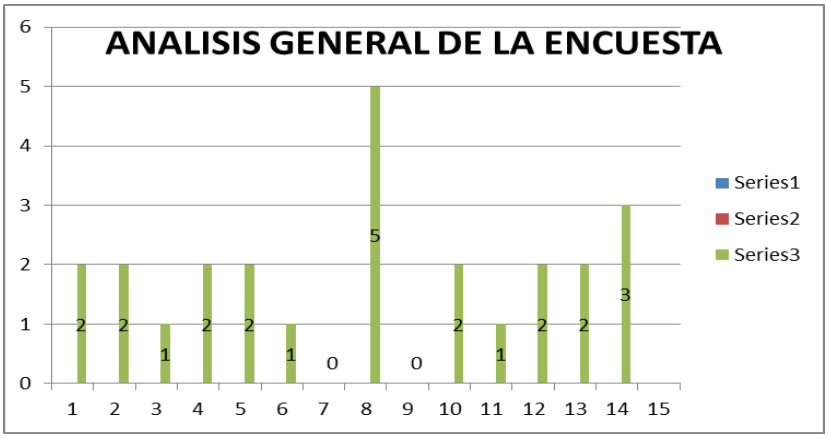


Tabla 2. ***Uscategui J.*** **(2014).** Grafico *Análisis General* ***de la encuesta*** **Recuperado el 24 septiembre de 2014**

Análisis a la primera pregunta

1	¿Cuáles son las fallas más comunes de su computador en Disemeq?	A. Problemas de antivirus o licencias	2
		B. lento el equipo y problemas de software	2
		C. ninguna	1

Tabla 3. ***Uscategui J.*** **(2014).** ***Datos de la primera pregunta*** **Recuperado el 24 septiembre de 2014**

Cuerpo del proyecto

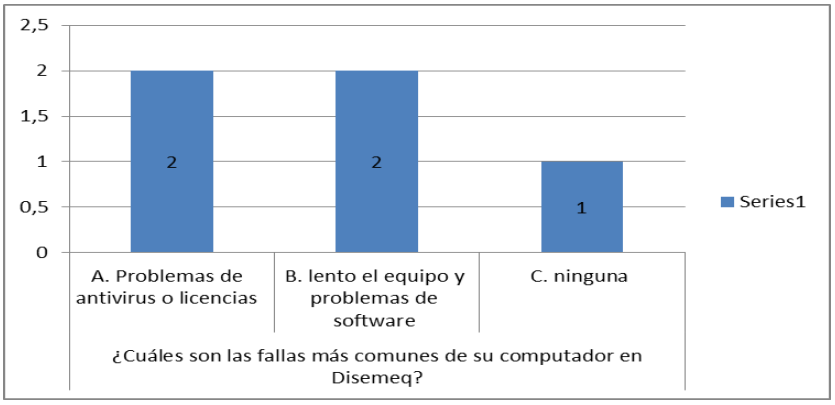


Tabla 4. ***Uscategui J.*** **(2014). Grafico** ***Análisis a la primera pregunta*** **Recuperado el 24 septiembre de 2014**

Análisis a la segunda pregunta

2	Cómo archiva u organiza la información de su computador en Disemeq Ltda?	A. En carpetas y archivos	2
		B. En CD, Discos duros, Memoria USB	2
		C. ninguna	1

Tabla 5. ***Uscategui J.*** **(2014).** ***Datos de la segunda pregunta*** **Recuperado el 24 septiembre de 2014**

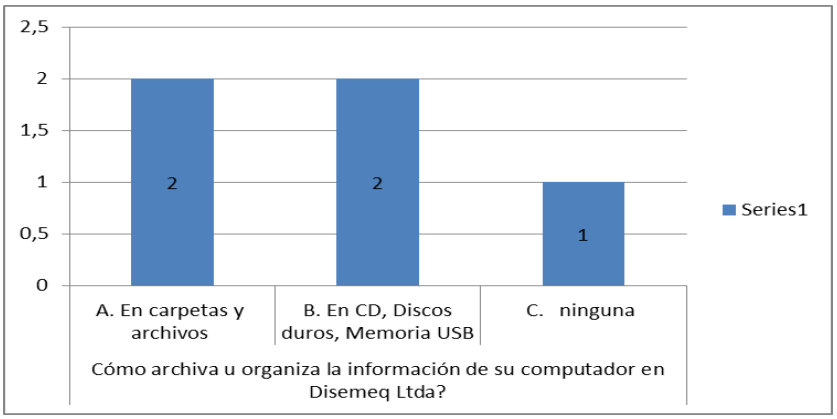


Tabla 6 ***Uscategui J.*** **(2014). Gráfico de** ***Análisis a la segunda pregunta*** **Recuperado el 24 septiembre de 2014**

Análisis a la tercera pregunta

3	¿Sabe usted si Disemeq Ltda, tiene políticas de seguridad informática para proteger la información?	A. SI	0
		B. NO	5
		C. No sabe	0

Tabla 7. ***Uscategui J.*** **(2014).** ***Datos de la tercera pregunta*** **Recuperado el 24 septiembre de 2014**

Cuerpo del proyecto

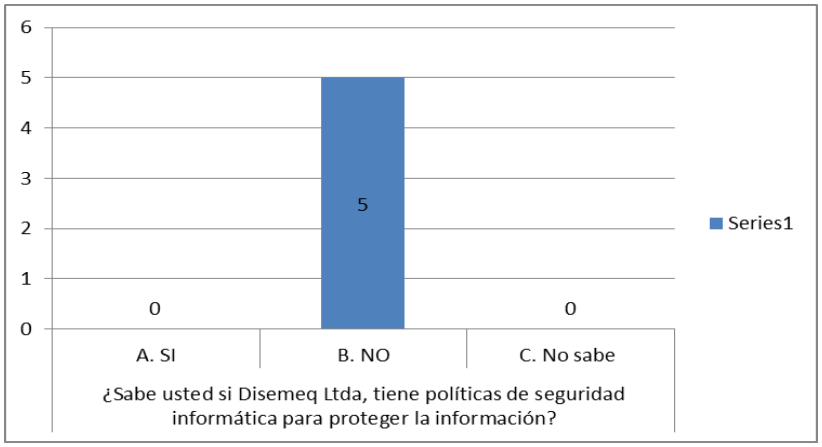


Tabla 8 ***Uscategui J.*** **(2014).** ***Gráfico de Análisis a la tercera pregunta*** **Recuperado el 24 septiembre de 2014**

Análisis a la cuarta pregunta

4	¿Qué tipo de seguridad implementa para proteger su computador?.	A. Por medio de contraseñas	2
		B. coloca contraseña a los archivos del computador	1
		C. ninguna	2

Tabla 9. ***Uscategui J.*** **(2014).** ***Datos de la cuarta pregunta*** **Recuperado el 24 septiembre de 2014**

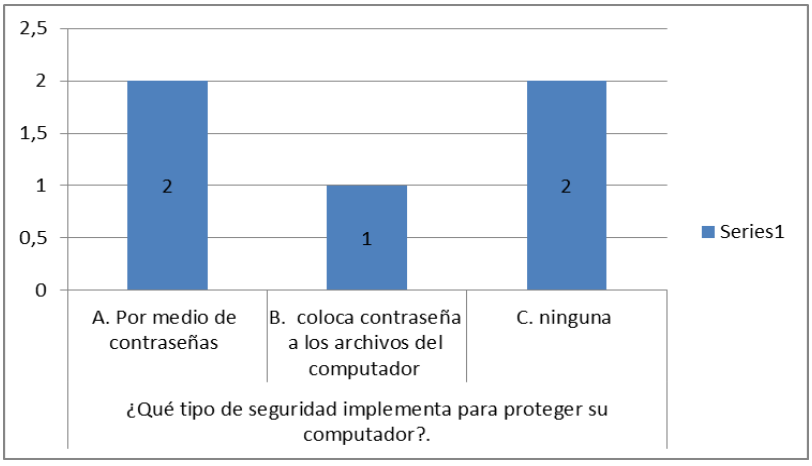


Tabla 10 ***Uscategui J.*** **(2014).** ***Gráfico de Análisis a la cuarta pregunta*** **Recuperado el 24 septiembre de 2014**

Análisis a la quinta pregunta

Cuerpo del proyecto

5	¿visita usted con frecuencia las redes sociales dentro de Disemeq para buscar alguna información?.	A. SI	2
		B. NO	3

Tabla 11. ***Uscategui J.*** **(2014).** ***Datos de la quinta pregunta*** **Recuperado el 24 septiembre de 2014**

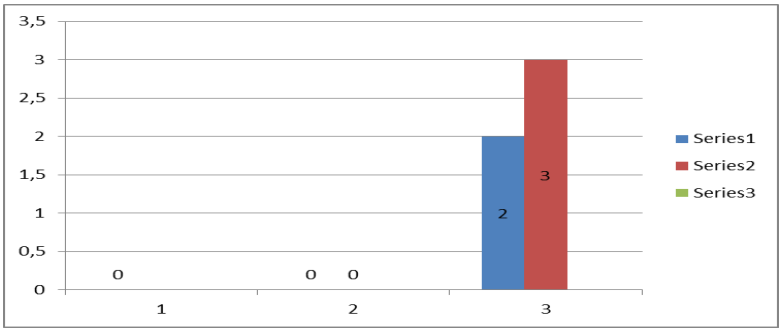


Tabla 12 ***Uscategui J.*** **(2014).** ***Gráfico de Análisis a la quinta pregunta*** **Recuperado el 24 septiembre de 2014**

Según las preguntas hechas a los empleados de la empresa Disemeq Ltda, vemos que las fallas más comunes son la lentitud de los computadores; se archiva u organiza la información en carpetas y archivos pero esto es un error porque se vez llegue a tener ataques informáticos la información corre bastante riesgo de perderse; también vemos claramente que Disemeq Ltda, no tiene políticas de seguridad informática para proteger la información; la seguridad que implementan los empleados por medio de contraseñas a sus equipos es muy básica y no cumple con los estándares según la norma ISO / IEC 27001 para proteger la información; además vemos que visitan con frecuencia las redes sociales dentro de Disemeq esto hace que normalmente bajemos virus informáticos y puede dañar nuestra información.

Cuerpo del proyecto

13. Fase 1: Caracterización de la infraestructura actual de la red implementada en Disemeq Ltda.

Disemeq cuenta con una red doméstica de 22 computadores instalados, con una topología tipo estrella, con una red cableada de 8 equipos conectados por medio de un Switch marca Trendnet de 32 puertos distribuidos por cable UTP de nivel 4, por todo el edificio construido hace aproximadamente 10 años, por lo que es mucho tiempo de estar instalados estos cables ya que la vida útil del cable UTP es de aproximadamente 5 años. Por otra parte tenemos una red inalámbrica (WIFI) de 14 computadores portátiles, los cuales se encuentran conectados mediante un router inalámbrico marca Trendnet de 4 puertos de capacidad de 80 metros de alcance, la capacidad de ancho de banda es 2 megabyte por segundo en rehusó, suministrada por el operador ISP Movistar, la mayoría de los equipos de conexión están incrustados en un gabinete de 65cmx40cmx40cm en metal, ubicados debajo de la escalera en un cuarto muy estrecho con poca ventilación, sin aire acondicionado, expuestos al polvo, también se guardan los elementos de aseo de la empresa, lo cual es inadecuado porque lleva humedad a todos los equipos.

Cuerpo del proyecto

También posee un circuito cerrado de televisión con 8 cámaras marca walcon para la seguridad física del edificio. Decimos que es una red doméstica porque no posee ninguna protección de seguridad informática, ya que no cumple con la norma mínima de protección, como lo hemos dicho no posee un firewall para filtrar el acceso, ni los computadores, no dispone de un antivirus que proteja la red y su información está a la merced de los piratas, esto es muy peligroso tratándose de una información tan delicada y valiosa, tampoco dispone de un servidor que administre el acceso y los computadores.

El ancho de banda de Disemeq Ltda, es de 2048 Mbps.

Test de Velocidad de claro en la empresa

Ilustración 3. *DISEMEQ Ltda, Test de Velocidad de Claro* Recuperado el 15 de julio de 2014 en *Disemeq Ltda.*

Cuerpo del proyecto

A continuación se describe cada equipo y la función que ejecuta dentro de la empresa:

Los equipos que a continuación relacionamos se utilizan en la empresa Disemeq Ltda, para la conexión de toda la red de los 22 computadores.

EQUIPOS DE CONEXIÓN DE RED			
ITEM	***NOMBRE DEL EQUIPO***	***CARACTERISTICAS***	***DESCRIPCIÓN***
1	SWITCH	Marca: TRENDnet Puertos: 32 Modelo: TE100-S32+	Tomar la señal de internet de movistar y la distribuye por cable la red a 9 puntos.
1	Router inalámbrico	Marca: TRENDnet Puertos: 4 Modelo: TEW-452BRP	Tomar la señal del Switch por cable y la distribuye por WIFI a 14 puntos.
1	Moden wifi ADSL BHS	Marca: Movistar Puertos: 4 Modelo:1303	Es el encargado de bajar la señal de internet y llevarla al switch para su distribución

Tabla 13 Disemeq Ltda, *Equipos de conexión de la red* Recuperado el 20 de septiembre de 2014.

Los equipos que relacionamos a continuación se utilizan en Disemeq Ltda, para la vigilancia interna y externa de la parte física del edificio.

EQUIPOS DEL CIRCUITO CERRADO DE TELEVISIÓN			
ITEM	***NOMBRE DEL EQUIPO***	***CARACTERÍSTICAS***	***DESCRIPCIÓN***
1	Cámara	Marca: WALCON	Están distribuidas por todo el edificio en sitios estratégicos

		Modelo: N/A	para captar cualquier movimiento sospecho dentro y fuera de la empresa.
1	Monitor de 17”	Marca: Samsung Modelo: TRS 356987D2	Es el encargado de proyectar todo lo que se ve en todas las cámaras.
1	NVR IP	Marca: Modelo:	Este equipo se llama network video record es el encargado de grabar todos los video que capturan las cámaras

Tabla 14 **Disemeq Ltda, *Equipos del circuito cerrado de televisión* Recuperado el 20 de septiembre de 2014**

El equipo que presentamos a continuación se utilizan en Disemeq Ltda, para el control de acceso físico de personas visitantes al edificio.

SISTEMA DE CONTROL DE ACCESO DE VISITANTES			
ITEM	***NOMBRE DEL EQUIPO***	***CARACTERÍSTICAS***	***DESCRIPCIÓN***
1	Video-citofono:	Compuesto por una cámara, un teléfono, un parlante	Dispositivo que sirve para controlar el acceso de personas visitantes al edificio.

Tabla 15. Disemeq Ltda, *Sistemas de Control de Acceso a visitantes* Recuperado el 20 de septiembre de 2014

Cuerpo del proyecto

Los equipos de cómputo que relacionamos a continuación son utilizados en la empresa Disemeq Ltda, para ejecutar las labores diarias de los empleados que actualmente trabajan en la empresa.

EQUIPOS DE CÓMPUTO CONECTADOS			
ITEM	***NOMBRE DEL EQUIPO***	***ÁREA***	***DESCRIPCIÓN***
1	CALIDAD	Sistemas integrados de gestión	Custodio Castillo, es el director de sistemas integrados de gestión, red cableada
2	QHSE		Custodio Castillo, es el director de sistemas integrados de gestión, red cableada
3	COMPRAS	Compras y contratación	Liliana herrera, es la profesional de compras, red cableada
4	CONTABILIDAD	Contabilidad	Maribel Rivas, es la asistente de Gerencia, red cableada
5	MANTENIMIENTO	Logística	Dalmar Padilla, Director de Logística, red cableada
6	BODEGA		Alejandro Ortega, es el almacenista, red cableada
7	GERENCIA	Gerencia	Ramón Moreno, es la cabeza principal de la organización, red por WIFI
8	LICITACIONES		Anderson Daza, encargado de diseñar proyectos, red por WIFI

Cuerpo del proyecto

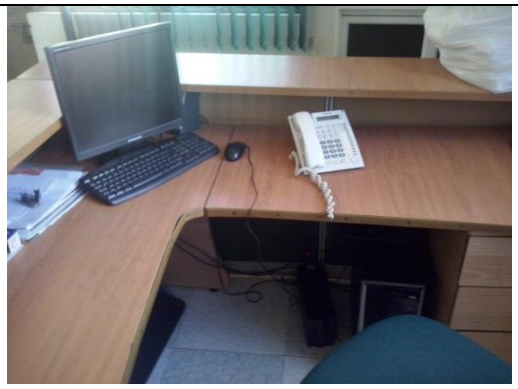
9	DIRECCION DE PROYECTOS	Proyectos	Diego Moreno, es el supervisor y coordinador de los proyectos, red por WIFI
10	SCANSERVER		TODOS, lo usan para guardar información y compartirla por toda la red, red cableada
11	SCANSERVER 2		TODOS, lo usan para guardar información y compartirla por toda la red, red cableada
EQUIPOS EN ARRIENDO			
12	SUPERVISORA HSE	Sistemas integrados de gestión	Yenifer Ortiz, su cargo es supervisora HSE, Red WIFI
13	SUPERVISOR QA-QC		José Luis corredor, su cargo es Supervisor QA-QC, red WIFI
14	SUPERVISORA HSE		Brenda infante, el cargo Supervisora HSE, red WIFI
15	SUPERVISOR HSE		Marlon Castellanos, el cargo es Supervisor HSE, red WIFI, Descripción la red es muy inestable en cuanto a conexión, sugerencia los formatos se manejaran vía web.
16	SUPERVISOR HSE		Darwin Hurtado, , el cargo es Supervisor HSE, red WIFI
17	CADENERO		Reinel Arévalo, el cargo es Cadenero, red WIFI
18	SUPERVISOR MECANICO		Jaime Ferreira, el cargo es Supervisor mecánico, red WIFI
19	TOPOGRAFO		Freider Molina, el cargo es

Cuerpo del proyecto

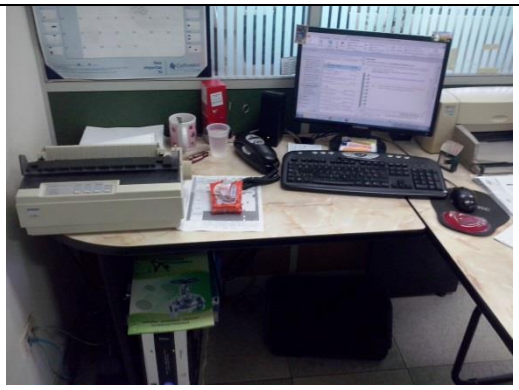
		Proyectos	topógrafo Red WIFI.
20	PROGRAMACION		Laura Cábulo, el cargo de Programación, Red WIFI.
21	INGENIERO RESIDENTE		Leonardo Moreno, ingeniero residente, Red WIFI
22	DIRECTOR DE OBRA		Wilfran Ramos, el cargo es Director Obra, Red WIFI

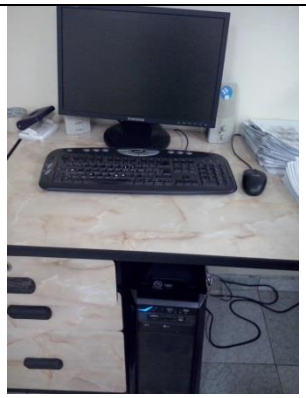
Tabla 16. Disemeq Ltda, *Equipos de cómputo de los empleados de Disemeq* Recuperado el 20 de septiembre de 2014

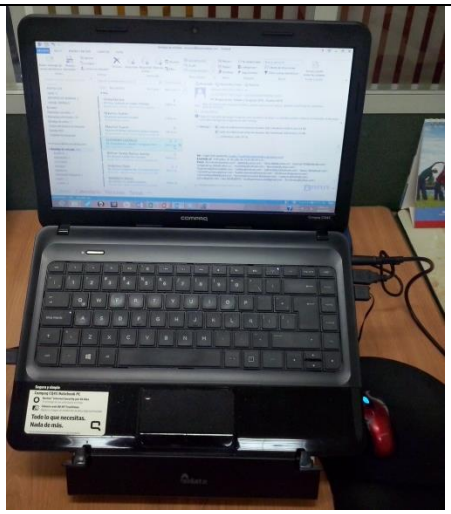
A continuación relacionamos unas fotografías tomadas en la empresa Disemeq Ltda, a los equipos que actualmente están en funcionamiento. Donde encontramos el equipo de la recepción, las impresoras, los equipos de área administrativa, los equipos de conexión a las red, los equipos de control de acceso al público, el circuito de cámaras de vigilancia y el gabinete donde se están alojados los equipos de conexión de toda la red.

FOTOGRAFÍAS DE LOS EQUIPOS QUE ESTÁN FUNCIONANDO ACTUALMENTE	
	

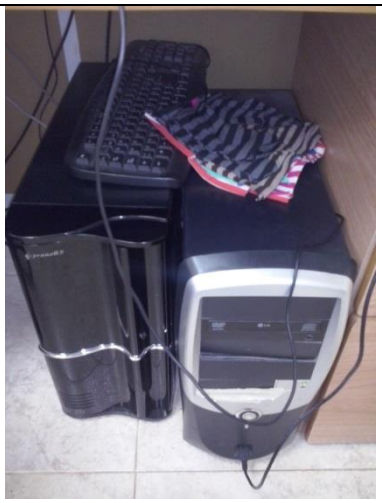
Cuerpo del proyecto







Cuerpo del proyecto



Cuerpo del proyecto

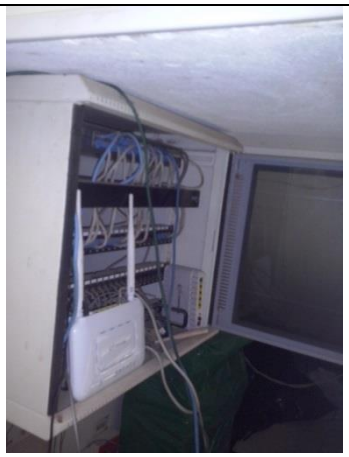
	
	

Tabla 17. Disemeq Ltda, *Fotografías tomadas de los Equipos de cómputo conectados actualmente* Recuperado el 20 de septiembre de 2014

13.1 EL SOFTWARE

El software que se maneja los portátiles y en los computadores de escritorio todos tienen Windows 7 y 8 solo tienen licenciamiento 8 de los 22, y el software aplicativo no tiene licenciamiento como es el paquete office (Word, Excel, powerpoint, access), el autocad, lo cual es nocivo para la empresa por no acatar lo dispuesto en LEY 603 DE 2000, por la cual se modifica el artículo 47 de la Ley 222 de 1995, sobre software ilegal en Colombia.

Por otra parte los computadores no tienen un antivirus licenciado ya que poseen antivirus gratis (AVAST, AVG) lo cual protege pero muy básico y no es igual como

si fuera un antivirus que cubra todos los protocolos de seguridad como las diferentes formas de ataques a los equipos.

Otro software que manejan en Disemeq está el **SIESA 8.5** es un software contable y lo ejecutan por acceso remoto pero este está muy bien protegido ya que es distribuido por la empresa en diferentes ciudades y esta albergado en un servidor con todos los protocolos de seguridad. Como también está el correo electrónico de Microsoft Outlook que cumple con todos los lineamientos de seguridad porque está en el mismo servidor y cada usuario posee su contraseña de seguridad para acceder al correo ya sea por página web o por el software Outlook.

Software contable SIESA version 8.5

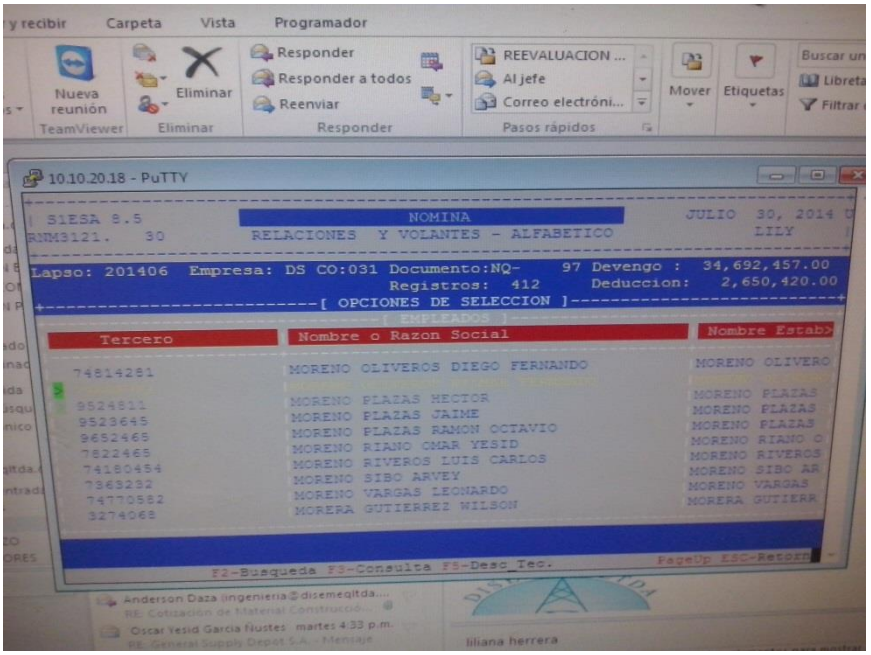


Ilustración 4. Disemeq Ltda, *Software siesa 8.5 de Disemeq Ltda.* Recuperado el 15 de julio de 2014

Cuerpo del proyecto

En Disemeq existe un sistema de seguridad y control de acceso tanto para los visitantes como también para los empleados, con el fin de darle seguridad a la parte física del edificio y evitar intrusos, asaltos, o sufrir de algún tipo de ataque informático.

Distribución de la Red actual en DISEMEQ

Red actual en Disemeq Ltda Piso 1

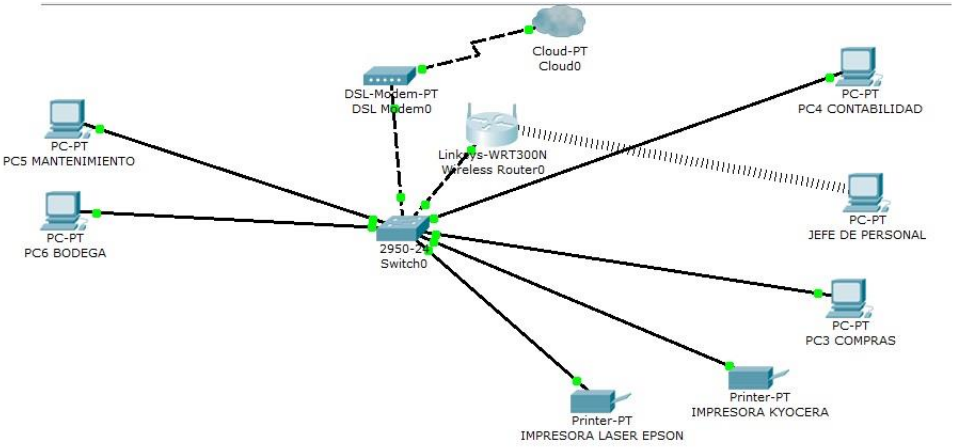


Ilustración 5. **DISEMEQ Ltda, *Red actual en Disemeq Ltda Piso 1* Recuperado el 15 de julio de 2014**

Red actual en Disemeq Ltda Piso 2

Cuerpo del proyecto

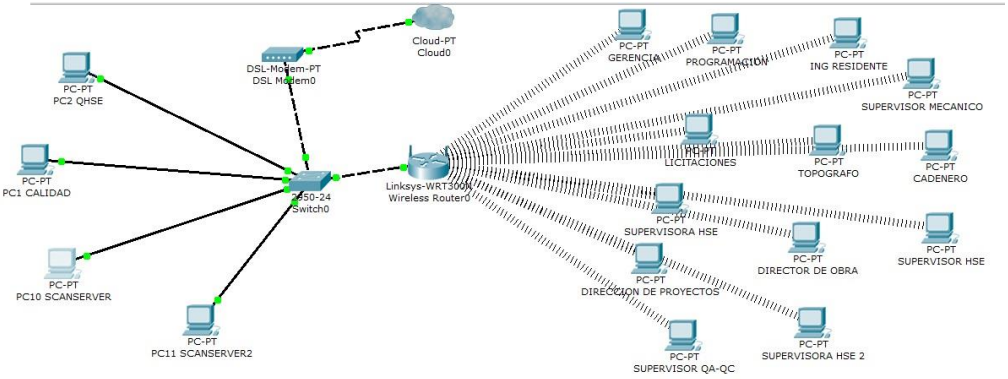


Ilustración 6. **DISEMEQ Ltda, *Red actual en Disemeq Ltda Piso 2* Recuperado el 15 de julio de 2014**

14. Fase 2. Determinación de las amenazas e impactos sobre la infraestructura de la red.

Al determinar las amenazas y entender los impactos que producen es cuando nos damos cuenta que en una empresa es muy importante proteger nuestra información y blindarla contra cualquier ataque de la red, es por eso muchas fallas en los sistemas informáticos son atribuidos a errores de los usuarios, ya que a veces se convierten en el eslabón más débil de la cadena de protección de la información digital, es a través de las personas, que los inescrupulosos acceden a los sistemas informáticos y pueden ingresar a realizar delitos.

Las principales amenazas e impactos que se presentan:

- En primer lugar se tiene que la red fue implementada hace más de 5 años, y su red cableada es tiempo de cambiarla porque ya cumplió su vida útil.

Cuerpo del proyecto

- La red implementada es domestica (plana) sin ninguna seguridad, ya que no posee un firewall (es un software o hardware basado en seguridad de la red del sistema que controla el tráfico de red entrante y saliente en base a un conjunto de reglas aplicadas).

- Los equipos que se encargan de interconectan la red están en sitio no adecuado ya que se alojan debajo de la escalera y el cuarto es muy reducido de difícil acceso y sin ventilación apropiada según las normas.

- No posee un servidor que administre toda la red, y la información que se maneja de la empresa no está organizada, controlada, ni supervisada lo que puede generar pérdida parcial o total.

- El software utilizado en los equipos de cómputo no cumple por lo criterios de ley software legal ya que en la mayoría de los equipos no tiene licencia.

- El uso de claves con bajo nivel de seguridad, fáciles de descubrir donde algunos usuarios utilizan claves tan simples como su propio nombre, nombre de familiares, un número de teléfono, el número de identificación, o cualquier otro que hace muy fácil el descubrirlo e incluso sin clave de acceso.

- Se autoriza permiso de conexión de dispositivos a otras personas, muchas veces por confianza o por “hacerle un favor” a otra persona, se deja que se conecten dispositivos, que sin saberlo el usuario, pueden traer “troyanos” que van a permitir huecos de seguridad ya que algunas veces no se detectan por los antivirus.

- Los usuarios no hacen revisión de antivirus y anti-spam frecuentemente, muchos usuarios “se cansan” de estar usando el antivirus o los programas

de protección y no lo ejecutan muy frecuentemente, con lo cual abren huecos de seguridad en los sistemas informáticos.

- Los usuarios no realizan copias de seguridad a tiempo, muchas veces, los usuarios, se confían de los datos que tienen almacenados y solo cuando sufren la pérdida irrecuperable, es cuando se dan cuenta que estar actualizando las copias de seguridad les permitiría recuperar la información.

- Los usuarios hacen configuraciones e instalaciones sin permisos, es común encontrar usuarios que consideran que pueden configurar o modificar aplicaciones sin consentimiento y pueden generar problemas como pérdida de información, permiso de acceso no autorizado, desinstalación de software propio o danos a las aplicaciones de la empresa.

- En Disemeq no hay control de acceso a las redes sociales, páginas de pornografías, páginas de juegos, páginas que ofrecen música, ya que en estas páginas abundan los malware, virus, es altamente peligroso descargar algún tipo de archivo.

  En Disemeq no hay autenticación de usuarios ya que no hay control de acceso a la información.

- Otro tipo de amenazas del personal externo son: hackers, Gurus, Lamers o Script-Kidders, CopyHackers, Bucaneros, Newbie, Wannaber, Samurai, Piratas Informáticos, Creadores de Virus.

- Otras Amenazas por Personal Interno tales como: Ex-Empleado, Curiosos, Terroristas, Intrusos remunerados. Estas personas pueden tomar la información y comercializarla al mejor postor, donde toman esta información hacen provecho monetariamente haciendo delitos como suplantación de

identidad, comercialización de los servicios con ventas ficticias y le pueden dañar la imagen de la empresa.

15. Fase 3. Analizar la vulnerabilidad y determinar la calidad de los controles o servicios de seguridad.

La red de computadores en Disemeq Ltda, se encuentra mal segmentada, porque no cumple con la norma ISO/IEC 27001 y se debe implementar seguridad informática, colocando un firewall que se encargue de administrar el tráfico de la red tanto entrante como saliente, también adquirir e implementar un servidor para la administración de todos los computadores como también la información que se maneja de la empresa para organizada, controlarla, supervisarla y darle protocolos de seguridad de accesibilidad a todos los usuarios, que el servidor junto con el firewall trabajen en conjunto, estas son las vulnerabilidades más necesarias para implementar la seguridad de la información.

Los equipos que interconectan la red deben estar en un cuarto con buena ventilación, libre del polvo, la humedad, el sol, y adecuado en un lugar amplio que con restricción de acceso a personas ajenas a los administradores de red.

Cuerpo del proyecto

La empresa debe adquirir software legal para cumplir con los estándares que se establecen en la Ley 44 de 1993[7] (Colombia aprende. 2014). y fue complementada en la ley 603 DE 2000, por la cual se modifica el artículo 47 de la Ley 222 de 1995, sobre software ilegal en Colombia.

Una vez se implemente y se estructure la red bien segmentada se debe realizar una capacitación, donde se le enseñe a los a usuarios a crear claves seguras, a utilizar protocolos de seguridad, y los mínimos requisitos que deben tener en cuenta para la utilización de la red dentro de la organización y evitar infiltraciones a la red.

Una vez sea adquirido un firewall se realizara un filtrado de contenidos donde se llevara el control de acceso a redes sociales, páginas de pornográficas, páginas de juegos, páginas de música, ya que en estas páginas abundan los malware, virus, etc.

Los frecuentes ataques que sufre son por causa de virus informáticos, como los caballos de troya, rootkits, etc, desactualización de software como las actualizaciones automáticas, malware como programas que se encargan de manipular el sistema operativo Windows dejar abiertos los puertos para que entren intrusos sin autorización, la falta de control de las redes sociales esto ocasiona bajar virus o malware con toda libertad.

[7] http://www.colombiaaprende.edu.co/html/docentes/1596/article-73576.html#h2_2

Cuerpo del proyecto

16. Fase 4. Gestión de riesgos

Viendo en Disemeq Ltda, que cuenta con una red muy plana lo que debemos es en primer lugar es segmentar la red, los computadores que están conectados por cable le vamos a colocar una dirección IP que identifique cada uno de ellos en la red con el nombre del cargo que tiene cada usuario y los computadores portátiles también le vamos a colocar una IP nombrados tal como es el cargo de cada usuario, se debe hacer compra de un firewall que haga el filtrado de contenido de toda la red y adicionalmente se debe comprar un servidor que nos ayude a administrar la red donde le damos privilegios a cada usuario, dándole límites a cada uno y hasta donde tienen acceso. Con estos cambios se mejora la red un 90% además los computadores cableados debemos cambiar todo el cable, tomas y RJ45 ya que tiene mucho tiempo de uso, es obligatorio hacer cambio.

El equipo que baja la señal de internet pertenece operador isp nos corresponde segmentarlo con el equipo Router que da la señal de wifi para que trabajen distintos canales y no hagan conflicto al emitir la señal wifi.

Cuerpo del proyecto

Debemos construir un centro de cómputo donde esté libre de lluvia, humedad, calor, polvo, con buena ventilación, aire acondicionado y que tenga restringido el acceso a personas ajenas a la administración de la red o de la empresa, para colocar todos los equipos tanto los viejos como los que vamos a adquirir.

En cuanto al software que tienen los equipos, se debe comprar las licencias tanto de los sistemas operativos como los aplicativos para cumplir con lo dispuesto en LEY 603 DE 2000 sobre software legal. Se debe adquirir un antivirus licenciado con todas las protecciones que nos sirvan para combatir los virus y el malware que es el talón de Aquiles de todos los ataques informáticos.

El software contable **SIESA 8.5** se sigue manejando de la misma manera, ya que cumple con todos los estándares de seguridad por estar alojado en un servidor en la ciudad de Bogotá con todos los seguros para su navegabilidad. También de la misma manera está el correo electrónico de Microsoft Outlook que cumple con todos los lineamientos de seguridad porque está en el mismo servidor y cada usuario posee su contraseña de seguridad para acceder al correo ya sea por página web o por el software Outlook.

Cuerpo del proyecto

17. Fase 5. Entregar un manual (medio magnético) de las políticas de seguridad informática, lineamientos y uso de equipos dentro de la organización.

El manual de políticas de seguridad informática se incluirá como archivo adjunto en formato PDF, con todos los lineamientos necesarios para implementar seguridad en la empresa Disemeq Ltda. El enfoque este manual es capacitar al personal de la empresa y ponerlo práctica como política de seguridad dentro de la empresa.

18. Fase 6. Mostrar la simulación con un software

Se realizará una simulación en el software Paker Tracer de cómo se encuentra la red actualmente (red plana) diseñada y como debería segmentarse e implementarse con todos los protocolos de seguridad de una red ideal con las soluciones. Se entregara la simulación como archivo adjunto.

Cuerpo del proyecto

Distribución de la Red actual en DISEMEQ sin seguridad

La distribución que veremos a continuación está ubicada para el piso 1 y es donde se encuentra la parte administrativa de la empresa.

Distribución de la red actual piso 1

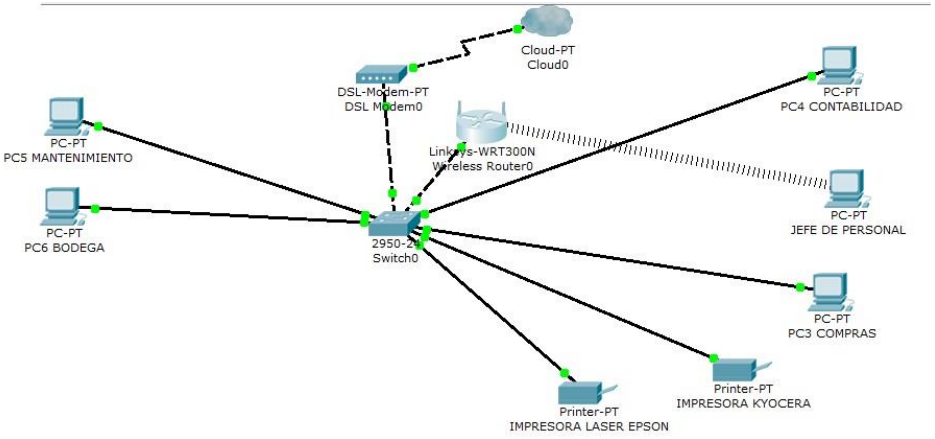


Ilustración 7. **DISEMEQ Ltda, *Red actual en Disemeq Ltda Piso 1* Recuperado el 15 de julio de 2014**

Cuerpo del proyecto

La distribución que veremos a continuación está ubicada para el piso 2 y es donde se encuentra la parte los empleados que realizan las licitaciones.

Distribución de la red actual piso 2

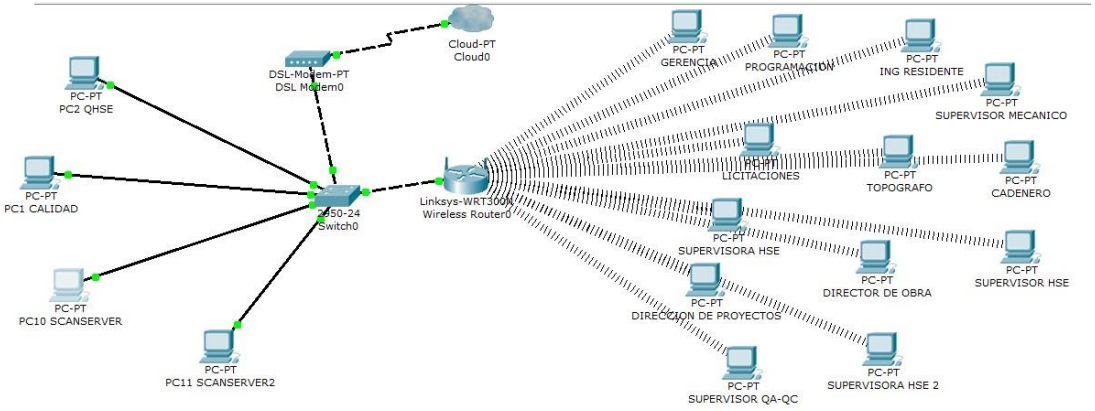


Ilustración 8. **DISEMEQ Ltda,** ***Red actual en Disemeq Ltda Piso 2*** **Recuperado el 15 de julio de 2014**

Red segmentada como debe implementarse en Disemeq Ltda.

La distribución que veremos a continuación, es como debe quedar implementada con todos los cambios para la red de computadores de Disemeq Ltda y así colocarle la seguridad informática a toda la empresa con el fin de proteger la información.

Cuerpo del proyecto

Distribución de la red a implementarse Piso 1

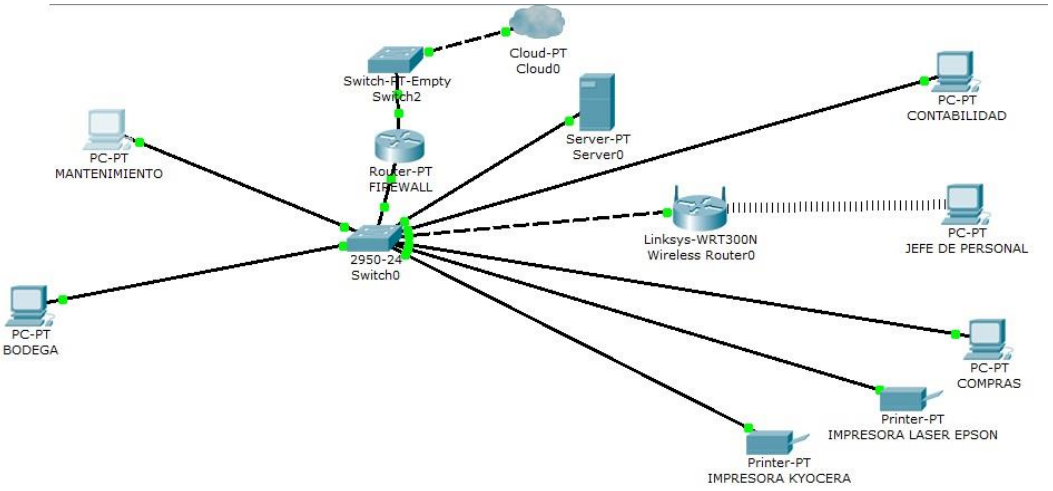


Ilustración 9. DISEMEQ Ltda, *Distribución de la red a implementarse Piso 1* Recuperado el 15 de julio de 2014

Distribución de la red a implementarse Piso 2

Cuerpo del proyecto

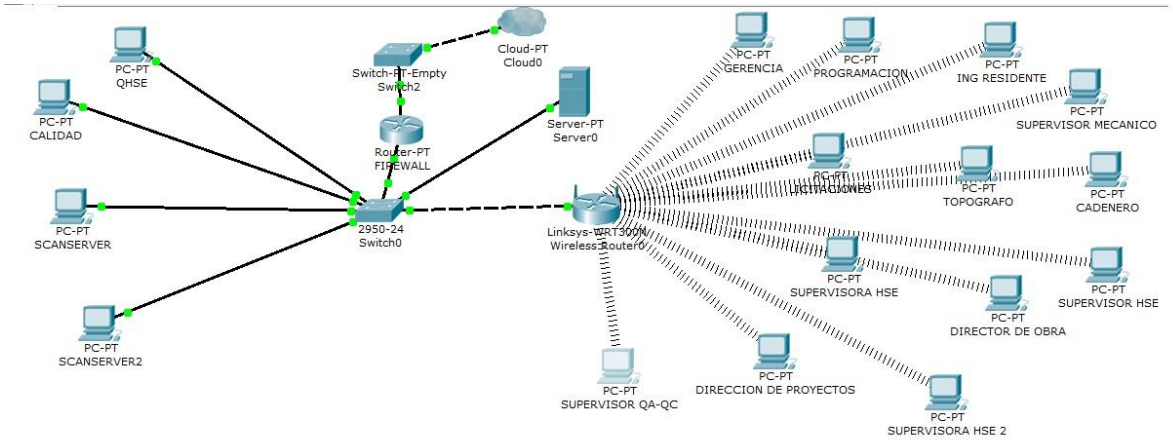


Ilustración 10. DISEMEQ Ltda, *Distribución de la red a implementarse Piso 2* Recuperado el 15 de julio de 2014

19. Fase 7. Realizar un documento que presente las soluciones que permitan aumentar y mejorar el nivel de seguridad de la información en Disemeq Ltda.

En esta fase se pretende dar las soluciones fundamentales necesarias para mejorar e implementar tanto la infraestructura de red como la protección de la información con la seguridad informática, por tales razones avanzaremos de acuerdo al orden fundamental de necesidad.

Reemplazo del cableado de red.

Cableado de red UTP Categoría Nivel 6

Ilustración 11. COMPUELTRO (2012) Recuperado de http://compueltro.blogspot.com/2012/05/switch-red-datos-cable-utp-cat6.html

Cuerpo del proyecto

La red cableada que conecta los computadores de escritorio en Disemeq Ltda, fue implementada hace más de 5 años, desde la compra del edificio, generalmente la vida útil del cable es de 5 años por lo que corresponde reemplazar el cable UTP que tiene nivel 5 por un cable UTP nivel 6, también los RJ5 y las tomas se debe cambiar para mejorar el transporte de transmisión de los datos.

Por otra parte para la conexión de los 22 computadores; los 8 cableados con conexión JR45 y los 14 por WIFI, se recomienda un ancho de banda de 5 megas dedicados o 10 megas en rehusó, para tener una navegabilidad óptima. Distribuyendo más o menos 512 kbps por equipo.

Seguridad de Equipos de cómputo.

Centro de cómputo implementado

Ilustración 12. Cuevas A. (2011) Cuarto de comunicación Recuperado de http://proyectoalezito.blogspot.com/

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos solo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios, para protegerlos se debe tener en cuenta que:

Cuerpo del proyecto

● La temperatura no debe sobrepasar los 18˚ C y el límite de humedad no debe superar el 65% para evitar el deterioro.

● Los centros de cómputo deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en este ámbito.

● Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

Disemeq no cuenta con un sitio bien adecuado para albergar los equipos que le dan servicio a la red, por lo tanto se debe acondicionar un sitio que nos de todas esta clases protecciones, Debemos construir un cuarto de máquinas donde esté libre de lluvia, humedad, calor, polvo, con buena ventilación, aire acondicionado y que tenga restricción de acceso de personas.

Segmentar la red

Imagen de una red técnicamente bien segmentada

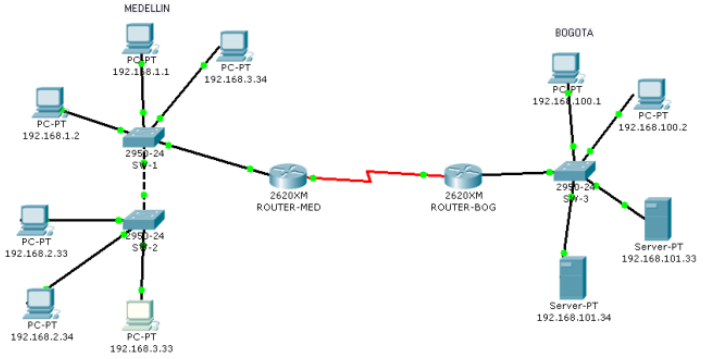


Ilustración 13. García J. (2012) *Topología de red* Recuperado de *http://6104info.blogspot.com/2012/06/administracion-de-redes-de-area-local_3482.html*

En Disemeq Ltda, cuenta con una red doméstica ya que no posee casi ninguna protección para la empresa, por lo que debemos segmentar la red, de la siguiente

manera: Los computadores que están conectados por cable se deben conectar por medio de una dirección IP que identifique cada uno de ellos en la red con el nombre del cargo que tiene cada usuario y los computadores portátiles también le vamos a colocar una dirección IP nombrados de la misma forma. Por lo que la red cableada estaría plenamente identificada, separada de la red inalámbrica. Como se muestra a continuación:

RED DISEMEQ A IMPLEMENTAR CON IP FIJA		
Nombre de la RED	**DISEMEQ_LTDA**	**192.168.2.1**
DESCRIPCION	CLASE DE RED	DIRECCIONAMIENTO IP
La red cableada se debe implementar no con DCHP (conexión automática) sino direccionamiento estático así:	El nombre del Switch es SW_PRINCIPAL y es el que se encarga de conectar los equipos cableados.	192.168.2.3 hasta el 192.168.2.100 con mascara de red 255.255.255.0 para los equipos por cable. Incluye una dirección para conectar Wireless Router que administra la red wifi.
La red inalámbrica o WIFI se debe implementar no con DCHP (conexión automática) sino direccionamiento estático así:	El nombre del Wireless Router es WIFI_DISEMEQ y es el que se encarga de conectar los equipos en red inalámbrica o WIFI.	192.168.2.101 hasta el 192.168.2.252 con mascara de red 255.255.255.0 para los equipos que van a ser conectados por Red inalámbrica o WIFI.

Tabla 18 Uscategui J. Direccionamiento IP a implementar en la *Red Disemeq* Recuperado el 25 de septiembre de 2014.

Adquisición de un firewall

Firewall estructurado e implementado

Cuerpo del proyecto

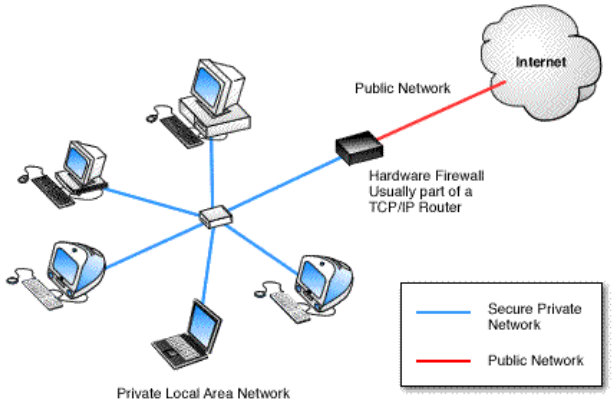


Ilustración 14. Vicomsoft Ltda (2011-2014) Recuperado de *http://www.vicomsoft.com/learning-center/firewalls/*

Se debe Adquirir un firewall donde haga filtrado de contenido, y denegué el acceso a quien no esté autorizado en toda la red se recomienda comprar un Vigor 2925 Dual-WAN Router Firewall o similar el cual implementa más seguridad, administración, el cual tiene las siguientes características: "Dual-WAN Gigabit Ethernet, Dual-WAN 3G / 4G (a través de módem USB), All-WAN funcionamiento simultáneo, Load-Balancing y Failover WAN, IPv6 Ready, Alto rendimiento - hasta 300Mb / s cortafuegos rendimiento, DrayTek Firewall con enorme flexibilidad, Conmutador de 5 puertos Gigabit Ethernet LAN, Monitoreo de temperatura (opcional termómetro), 802.11a / b / n de LAN inalámbrica (Vigor 2925n / n-plus), Banda dual (2,4 GHz / 5 GHz) Wireless (Vigor2925n-plus), Puertos de teléfono gemelo VoIP (con POTS conmutación por error), Wireless Portal Invitado, Múltiples subredes LAN Privadas, SMS (mensaje de texto) Alerta VLAN (Puerto o 802.1q basado), Multicast IGMP v2 y v3, Incluye SmartMonitor (50 usuarios), Filtrado de contenido (por palabra clave, tipo de datos o una categoría), Ethernet y WiFi VLAN (grupos comunes / distintas), Integración LDAP para VPN y acceso de los usuarios QoS (Layer 2 y 3, 802.1 y TOS / DCSP), Hasta 32 túneles VPN para LAN-to-LAN o tele trabajadores, VPN Canalizaciones y copia de seguridad SSL VPN - Túnel o Proxy (25 usuarios), Puerto USB para la impresora, registros o módem 3G Opcional Vigor Care Disponible"[8] (SEG DrayTek. 2013).

[8] http://www.draytek.co.uk/products/business/vigor-2925

Cuerpo del proyecto

Firewall Vigor 2925 Dual-WAN

Ilustración 15. SEG/DrayTek UK (2014) *Firewall Vigor 2925 Dual-WAN* Tomada de http://www.draytek.co.uk/products/business/vigor-2925

Al implementar este tipo de hardware (firewall) el hace control de contenido y filtrado de contenido, control de acceso a redes sociales, páginas de pornográficas, páginas de juegos, páginas que sean maléficas para nuestra navegabilidad, también hace administración de toda la red y mejorar al 90% la seguridad de la red.

Implementación de servidor LAN

Ilustración 16. IDLServicios.com (2009-2014) Implementación de servidor LAN Recuperada de *http://www.informaticamoderna.com/Servidor.htm*

Adicionalmente se debe adquirir un servidor que nos ayude a administrar la red donde administremos la red, dándole privilegios a cada usuario, y podamos alojar la información y así evitar pérdidas por mala administración. Con estos cambios se mejora la red, pero hoy en día es casi imposible no ser víctima de intrusos de quieran apoderarse de nuestra red. El servidor es “También llamado "Host" ó anfitrión; es una computadora con muy altas capacidades de proceso, encargada de proveer diferentes servicios a las redes de datos (una red es un conjunto de computadoras interconectadas entre sí), tanto inalámbricas como las basadas en cable; también permite accesos a cuentas de correo electrónico, administración de dominios empresariales, hospedaje y dominios Web entre otras funciones. Los servidores de preferencia se deben montar en gabinetes especiales denominados Racks, dónde es posible colocar varios Servers en los compartimientos especiales y ahorrar espacio, además de que es más seguro porque permanecen fijos.

Los servidores tienen sistemas que les permiten resolver ciertas averías de manera automática así como sistemas de alerta para evitar fallas en operaciones de datos críticos, ya que deben estar encendidos los 365 días del año las 24 horas del día. Actualmente para el uso dentro de redes pequeñas (casas y algunas oficinas), se pueden utilizan como servidores las computadoras de escritorio "Desktop", debido a que tienen la capacidad de soportarlas las funciones de manera eficiente a muy bajo costo; hasta el 80% de ahorro con respecto a un servidor comercial”[9] (Informática moderna 2014).

También podemos administrar todos los computadores y la información que se maneja de la empresa para organizada, controlarla, supervisarla y darles protocolos de seguridad de accesibilidad a todos los usuarios, esta

[9] http://www.informaticamoderna.com/Servidor.htm

implementación es la más importante para evitar las vulnerabilidades e implementar la seguridad de la información en Disemeq Ltda.

Implementación de VLAN en la empresa

Las VLANs "son agrupaciones, definidas por software, de estaciones LAN que se comunican entre sí como si estuvieran conectadas al mismo cable, incluso estando situadas en segmentos diferentes de una red de edificio o de campus. Es decir, la red virtual es la tecnología que permite separar la visión lógica de la red de su estructura física mediante el soporte de comunidades de intereses, con definición lógica, para la colaboración en sistemas informáticos de redes. Este concepto, fácilmente asimilable a grandes trazos implica en la práctica, sin embargo, todo un complejo conjunto de cuestiones tecnológicas. Quizás, por ello, los fabricantes de conmutación LAN se están introduciendo en este nuevo mundo a través de caminos diferentes, complicando aún más su divulgación entre los usuarios"[10] (Comunicaciones *World* nº 93 1995).

En Disemeq se debe implementar redes locales virtuales VLANs, sirven para controlar el tráfico de la información dentro de una red con distintas áreas, añadiendo funciones de conmutación, tienen software de gestión avanzado para dar privilegios a todos los usuarios y se hace a través de un servidor. Y su implementación se debe enfocar así:

Estructura de VLANs para implementar

[10] http://www.lcc.uma.es/~eat/services/rvirtual/rvirtual.html#link17

Cuerpo del proyecto

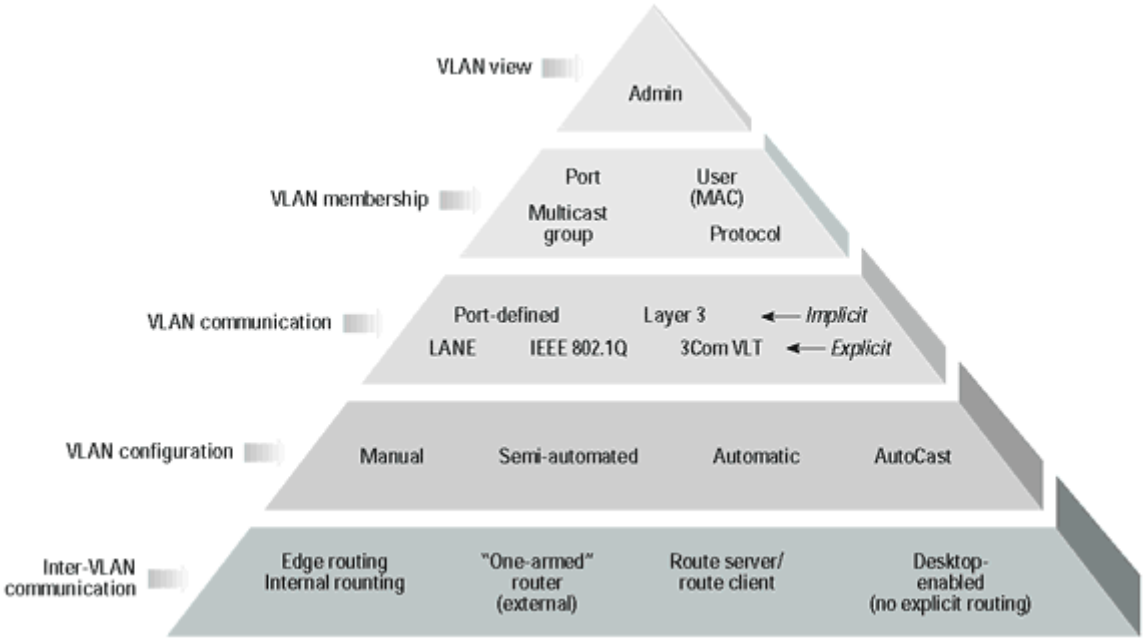


Ilustración 17. Comunicaciones World nº (1993) ***Estructura de VLANs para implementar*** **http://www.lcc.uma.es/~eat/services/rvirtual/rvirtual.html#link17**

Red implementada con VLANs

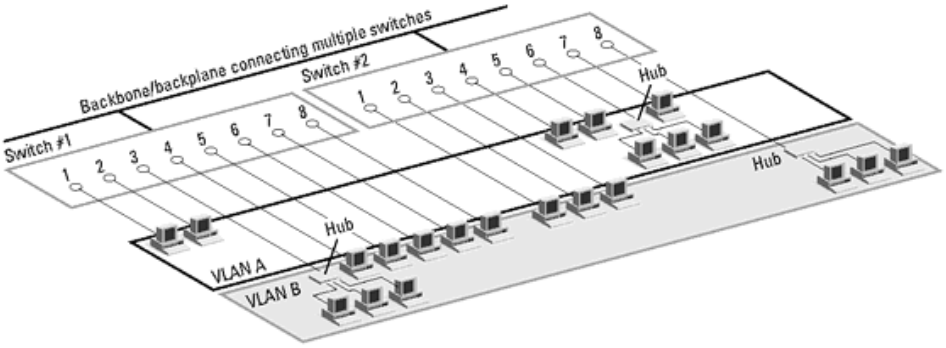


Ilustración 18. Comunicaciones World nº (1993) ***Red implementada con VLANs*** **http://www.lcc.uma.es/~eat/services/rvirtual/rvirtual.html#link17**

Implementación de un Directorio Activo

Cuerpo del proyecto

Imágen de un directorio activo (AD) implementado

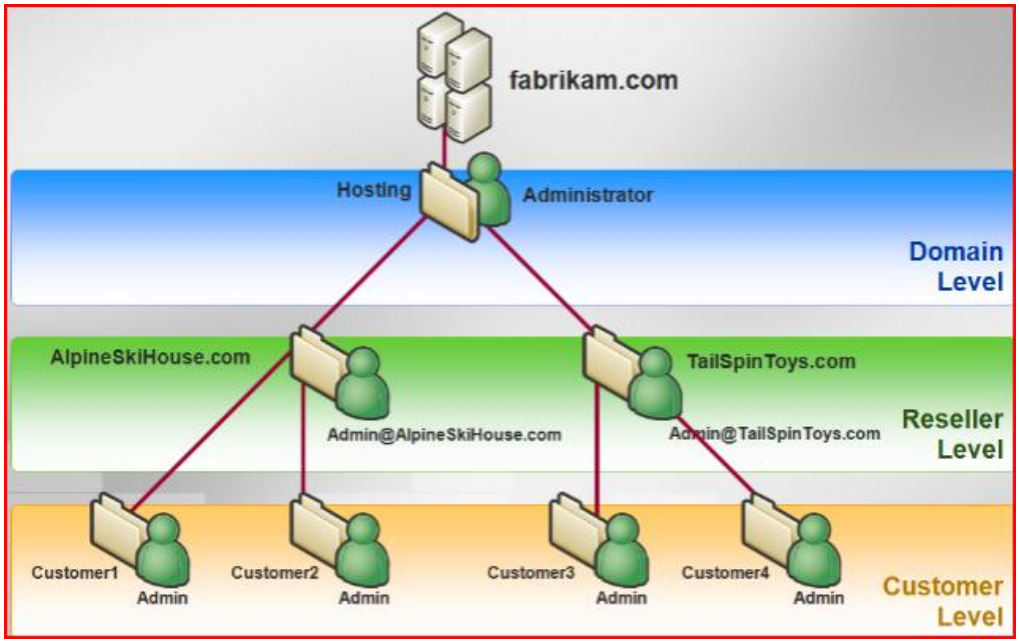


Ilustración 19. Microsoft Corporation (1993) *directorio activo (AD) implementado* Recuperado de http://blogs.technet.com/b/linacre/archive/2007/06/09/administraci-oacute-n-automatizada-para-hosters.aspx

Es el término usado para referirse a la implementación de servicio de directorio en una red distribuida de computadores, utiliza distintos protocolos (principalmente LDAP, DNS, DHCP, Kerberos, dependiendo del sistemas operativo con el que cuente el servidor, de forma sencilla se puede decir que “es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red, su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso”[11] (LinkedIn Corporation 2014). Se puedo utilizar y crear directorio activo en Windows, Linux, Macintosh, etc.

[11] http://www.slideshare.net/kwmitasdvf/actividad10-29126755

Cuerpo del proyecto

En Disemeq se debe implementar este tipo de administraciones una vez se tenga un servidor para el manejo de la red de datos de la empresa, con el fin de darle los diversos privilegios que tiene cada empleado según su cargo que ocupa en la empresa y según la información que vayan a manejar. Por otra parte no se da ningún proceso o secuencia de configuración para directorio activo en este proyecto porque depende del sistema operativo que se esté usando en el servidor que se vaya a adquirir.

Respaldo Online de la información

La información que poseen las empresas en el mundo, es el bien más preciado, pero ellos no lo dimensionan y no lo aprecian, hasta que no pierden información o sufren pérdida parcial o total de la misma y generalmente no es protegida como es debido, por esta razón es necesario realizar copias de seguridad en otra parte diferente que no sea en la misma organización, debido a esto hay servicios de empresas en TIC en el mundo encargadas de guardar, cuidar, encriptar y proteger la información de empresas que soliciten este servicio. Para el caso de Disemeq Ltda, sería muy importante proteger su información para evitar pérdidas parciales o totales que son el activo más importante de esta empresa.

Licenciamiento de Software

Cuerpo del proyecto

Ilustración 20. Actualicese.com (2011) *Licenciamiento de Software* http://actualicese.com/actualidad/2011/07/18/gobierno-reduce-retencion-a-titulo-de-renta-en-servicios-de-licenciamiento-o-uso-de-software/

El software que se maneje en una empresa, se debe comprar licenciado tanto de los sistemas operativos (Windows 7 y 8) como los sistemas aplicativos (Office 2007, 2010, autocad, etc.) empresas como la Microsoft, adobe, dan buenas ofertas para empresa pyme que quieran comprar licencias por paquetes a muy buen precio por tal razón es fácil adquirir licencias para cumplir con dispuesto en LEY 603 DE 2000 sobre software legal en Colombia. Ya que si las empresas no adquieren sus licencias tendrán las siguientes penalidades; “La Ley 44 de 1993 especifica penas entre dos y cinco años de cárcel, así como el pago de indemnizaciones por daños y perjuicios a quienes comentan el delito de piratería de software. Se considera delito el uso o reproducción de un programa de computador de manera diferente a como está estipulado en la licencia. Los programas que no tengan licencia son ilegales y es necesaria una licencia por cada copia instalada en los computadores. A partir del mes de julio de 2001, y gracias a la reforma hecha al Código de procedimiento penal, quien sea encontrado usando, distribuyendo o copiando software sin licencia tendrá que pagar con cárcel hasta por un período de 5 años.

Sin embargo, uno de los logros más importantes de la legislación colombiana en materia de protección de derechos de autor fue la Ley 603 de 2000, en la cual todas las empresas deben reportar en sus Informes Anuales de Gestión el

cumplimiento de las normas de propiedad intelectual y derechos de autor. La Dirección de Impuestos y Aduanas Nacionales (DIAN) quedó encargada de supervisar el cumplimiento de estas leyes, mientras que las Superintendencias quedaron responsables de vigilar y controlar a estas empresas. Con esto, quedó claro que la ley colombiana se endureció en el tema de la propiedad intelectual y los derechos de autor"[12] (Colombia aprende, 2014).

Adquisición de Antivirus licenciado

Ilustración 21. sanespa32 (2011) Mejor antivirus Recuperado de http://listas.20minutos.es/lista/el-mejor-antivirus-hasta-este-momento-287909/

Se debe adquirir un antivirus licenciado, con todas las protecciones que nos sirvan para combatir los virus y el malware que nos proteja de todos los ataques que sufrimos diariamente en internet. Hay muchas marcas y empresas que ofrecen este tipo de Software entre los más recomendados son: AVAST, AVIRA, ESET, Kaspersky, AVG, etc. Los encontramos desde los 20 dólares por equipo hasta licencias para varios equipos a más bajo costo.

[12] http://www.colombiaaprende.edu.co/html/docentes/1596/article-73576.html#h2_2

Cuerpo del proyecto

La solución más óptima para corregir todos los ataques sufridos a la empresa es adquirir un software antivirus totalmente licenciado enfocado hacia pyme y él se encarga de proteger la mayoría de ataques, junto con el FIREWAL que es clave para proteger y filtrar la información.

CAPACITACIÓN DEL PERSONAL DE DISEMEQ LTDA.

Ilustración 22. Instituto T. *Capacitación de Personal* Recuperada de *http://www.cet1.ipn.mx/Paginas/inicio.aspx*

Una vez se implemente la restructuración de toda la red, bien segmentada, se debe realizar una capacitación a todos los funcionarios de la empresa, donde se les haga conocer el manual de políticas de seguridad informática, y se oriente en varios ejemplos que son fundamentales y sencillos para estar protegidos tales como crear claves seguras, a utilizar protocolos de seguridad, y los mínimos requisitos que deben tener en cuenta para la utilización de la red dentro de la organización.

Cuerpo del proyecto

20. PRESUPUESTO DETALLADO PARA LA IMPLEMENTACION DE LA RED SEGMENTADA CON TODA LA SEGURIDAD INFORMATICA.

NOMBRE DEL PROYECTO	ACTIVIDADES A DESARROLLAR	UNIDAD DE MEDIDA	CANTIDAD	INSUMOS	VALOR UNIT	UNIDAD	CANT	2.014	2.015	TOTAL
	adquisicion de un ancho de banda por 10 megas de velocidad	megas	10	compra de ancho banda	50.000,00	Mega	10	500.000		
							Subtotal	**500.000,00**		**500.000**
	cableado de red UTP Categoria nivel 6			**Mano de Obra**						
				Instalacion de puntos cableados	12.000,00	UND	8	$ 96.000,00		
				Cable UTP nivel 6	1.600,00	ML	160	$ 256.000,00		
				toma de red	7.500,00	UND	16	$ 120.000,00		
				Conector RJ 45 Hembra	5.500,00	UND	16	$ 88.000,00		
							Subtotal	**560.000,00**	-	**560.000**
	Centro de cómputo implementado			Gabinete de piso metalico color negro ventilado 60cmX2000cmX110cm	3.250.000,00	UND	1	$ 3.250.000,00		
				UPS Regulada 2 KVA	1.800.000,00	UND	1	$ 1.800.000,00		
				Varios	2.000.000,00	UND	1	$ 2.000.000,00		
				Instalacion mano de obra de centro de computo	2.700.000,00	UND	1	$ 2.700.000,00		
							Subtotal	**9.750.000,00**	-	**9.750.000**
	Segmentar, configurar, organizar, la red			Mano de obra (instalacion y configuracion)	25.000,00	UND	22	$ 550.000,00		
							Subtotal	**550.000,00**	-	**550.000**
	Adquisicion de Firewall			Compra de firewall	1.300.000,00	UND	1	$ 1.300.000,00		
							Subtotal	**1.300.000,00**	-	**1.300.000**
DIAGNOSTICO DEL ESTADO Y NIVEL DE SEGURIDAD DE LA INFORMACIÓN VIGENTE EN LA EMPRESA DISEMEQ LTDA DEL DEPARTAMENTO DE CASANARE	Respaldo Online de la información	Servicio por mes	1	Respaldo Online de la información	825.000,00	UND	1	$ 825.000,00		
							Subtotal	**825.000,00**	-	**825.000**
	Adquisicion de Servidor			Compra de Servidor: Intel Xeon E5-2420v2/4GB/500GB HD/PERC H310/ iDRAC7 Express	6.800.000,00	UND	1	$ 6.800.000,00		
							Subtotal	**6.800.000,00**	-	**6.800.000**
	Configuracion de VLANs			Instalacion y configuracion de VLANs para 22 equipos con dos subredes	1.200.000,00	UND	1	$ 1.200.000,00		
							Subtotal	**1.200.000,00**	-	**1.200.000**
	Configuracion de directorio activo			Instalacion y configuracion de Directorio Activo	2.200.000,00	UND	1	$ 2.200.000,00		
							Subtotal	**2.200.000,00**	-	**2.200.000**
	Licenciamiento de Software Legal			Licencias de Windows	90.000,00	UND	22	$ 1.980.000,00		
				Licencias de Office 2010	120.000,00	UND	22	$ 2.640.000,00		
				Licencia de Antivirus	95.000,00	UND	22	$ 2.090.000,00		
				Instalacion de windows, Office 2010, Antivirus	70.000,00	UND	22	$ 1.540.000,00		
							Subtotal	**8.250.000,00**	-	**8.250.000**
	Capacitacion del personal			Capacitacion de politicas de seguridad informatica dentro de Disemeq	27.000,00	horas	20	$ 540.000,00		
							Subtotal	**540.000,00**	-	**540.000**
				PRESUPUESTO TOTAL GENERAL				**31.150.000**	-	**32.475.000**

Elaboro: **JUAN ANDRES USCATEGUI NIÑO**
Ingeniero de Sistemas

Tabla 19 **Uscategui J.** ***Presupuesto Detallado del Proyecto a implementar*** **Recuperado el 25 de septiembre de 2014.**

21. RECURSOS DISPONIBLES

21.1 Recursos Tecnológicos

Para poder llevar a cabo el proceso del desarrollo del diagnóstico se utilizará un equipo de cómputo de propiedad del autor del proyecto:

Portátil Toshiba de 15", las características físicas del equipo son: (Sistema operativo Windows 7 profesional, Memoria RAM de 4GB, Disco Duro de 1 TB, Unidad de DVD R/RW, Office 2010, Acrobat Reader, winrar, Paker Tracer, etc).

Este equipo de cómputo se utilizó para realizar el proceso de documentación del proyecto.

21.2 Recurso Humano

Este Proyecto "Diagnóstico del estado y nivel de seguridad de la información vigente en la empresa Disemeq Ltda del Departamento de Casanare – DISEINFORDI". Estuvo liderado por la ingeniera Edna Roció Bernal la cual tenía el cargo de directora del proyecto, y por la otra parte estuvo a cargo de ingeniero de sistemas Juan Andrés Uscategui Niño, quien fue el autor de dicho proyecto, egresado de la Universidad Nacional Abierta y a Distancia, desde el año 2010, él ha trabajado como coordinador de las Tecnologías de información y las comunicaciones para la Gobernación de Casanare, con amplia experiencia en mantenimiento de computadores.

Cuerpo del proyecto

El contacto de la empresa Disemeq Ltda, nos acompañó el señor Julián Acelas quien tiene el cargo del Jefe de personal donde nos ayudaba con la información que requeríamos para realizar todo este proceso.

21.3 Recursos Financieros

El desarrollo del proyecto necesito de unos aportes económicos que son fundamentales para llevar a cabo este proyecto.

Haciendo una recopilación de los requisitos y costos que se necesitaban y se implementarían en la elaboración de este diagnóstico, se determinó los siguientes valores:

PRESUPUESTO PARA LA REALIZACION DEL PROYECTO				
DETALLE	**DESCRIPCION**	**CANTIDAD**	**V. UNITARIO**	**TOTAL**
Equipos	Computador portátil, con procesador Core i7, memoria 4 GB, disco duro de 500 GB.	1	$2.000.000	$2.000.000
Software a utilizar	Instaladores de Paker Tracer 5.0, Software Windows 7 licenciado, Paquete Office 2010, acrobat reader, entre otros	4	$750.000	$3.000.000
material bibliográfico	Compra y acceso a la literatura o bibliografía	6	$83.333	$499.998
Conexión a internet	Conexión banda ancha 2 mega Bytes de conectividad	1	$45.000	$45000
OTROS	Transporte, Papelería, y otros gastos	10	$150.000	$1.500.000
			TOTAL PRESUPUESTO	**$7.044.998**

Tabla 20. Uscategui J. *Presupuesto para la realización del proyecto* Recuperado el 25 de septiembre de 2014

Cada una de las actividades planteadas se llevaran a cabo con totalidad, cumpliendo con los requerimientos de este trabajo, que al final se tuvo como resultado un informe que muestra el estado y nivel de seguridad informática en la empresa Disemeq y soluciones que permitan mejorar, fortalecer y mitigar los ataques o entradas maliciosas a través de la red a esta entidad.

Cuerpo del proyecto

CRONOGRAMA DE ACTIVIDADES

CRONOGRAMA DE ACTIVIDADES								
Nombre del Proyecto: PROPUESTA DEL ESTADO Y NIVEL DE SEGURIDAD DE LA INFORMACIÓN VIGENTE EN LA EMPRESA DISEMEQ LTDA DEL DEPARTAMENTO DE CASANARE								
Integrante: Juan Andrés Uscategui Niño		Fecha de Inicio del Proyecto: 03 de Marzo 2014						
		Fecha de final del Proyecto: 25 de Septiembre de 2014						
		AÑO 2014						
		MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE
Fase 1	Caracterización de la infraestructura actual de la red implementada en Disemeq Ltda.	x	x					
Fase 2.	Determinación de las amenazas e impactos sobre la infraestructura de la red.		x	X				
Fase 3.	Analizar la vulnerabilidad y determinar la calidad de los controles o servicios de seguridad.			x				
Fase 4.	Gestión de riesgos			x	X			
Fase 5.	Entregar un manual (medio magnético) de las políticas de seguridad informática, lineamientos y uso de equipos dentro de la organización.				X	X		
Fase 6.	Mostrar la simulación con un software especializado en redes (Packet Tracer) sobre la red de Disemeq Ltda, antes y después de realizar todo el analisis.						X	
Fase 7.	Realizar un documento que presente las soluciones que permitan aumentar y mejorar el nivel de seguridad de la información en Disemeq Ltda						x	X

Tabla 21 Uscategui J. *Cronograma de Actividades* Recuperado el 12 de marzo de 2014

Cuerpo del proyecto

CONCLUSIONES

Las principales dificultades que se tuvieron en la ejecución de este proyecto "Diagnóstico del estado y nivel de seguridad de la información vigente en la empresa Disemeq Ltda del Departamento de Casanare – DISEINFORDI". Fue que la empresa no cuenta con un profesional para esta área de sistemas que administre, y nos guiara para buscar los ataques que en Disemeq sucedía, otra de las dificultades fue que la empresa, no tiene información exacta de la parte de sistemas y la red por lo que nos correspondió verificar toda la red y la información para encontrar los problemas que estaban pasando.

Al realizar el diagnóstico del estado y el nivel de seguridad informática existente en la empresa Disemeq Ltda. Se encontraron varios errores, fallas, falencias, o por falta de conocimiento, se han hecho omisiones que están claramente dando vulnerabilidades que hacen que la infraestructura de red y la seguridad informática tenga muchos ataques informáticos tanto a la parte de hardware como de software.

Se realizó un manual de las políticas de seguridad informática, lineamientos y uso de equipos dentro de Disemeq Ltda, el cual debemos poner en práctica todas las personas de la empresa y con el fin evitar futuros ataques informáticos.

Se realizó la simulación en el software (Packet Tracer) versión 5.0 del estado actual de toda la infraestructura de red, y como vemos hay varias fallas que están ocasionando ataques informáticos; por otra parte en este mismo software, se da la solución de cómo se debería implementar la infraestructura de red, según las normas ISO / IEC 27001, para evitar intrusos que dañen la red.

Al determinar el diagnóstico del estado y nivel de seguridad informática de la empresa Disemeq Ltda, se buscaron las soluciones que permitirán mejorar la

seguridad tanto en la infraestructura de red como en el nivel de seguridad informática.

Por último el aporte más significativo que se tuvo en este proyecto “Diagnóstico del estado y nivel de seguridad de la información vigente en la empresa Disemeq Ltda del Departamento de Casanare – DISEINFORDI” fue que dimos las soluciones definitivas al problema de la infraestructura de la red, tanto a nivel de software como de hardware y la administración, distribución, segmentación de toda la red para reducir dicha problemática al mínimo, sobre la seguridad informática en Disemeq Ltda.

Cuerpo del proyecto

BIBLIOGRAFÍA

Salazar, S. (2012). *Estado del Arte de La Seguridad Informática.* Cúcuta, Colombia: Universidad Francisco De Paula Santander.

ICONTEC. (icontec) *Compendio tesis y otros trabajos de grado, Norma 1486 Quinta actualización. 2010* Bogotá: Icontec.

González, Y. (2012). *Modulo Fundamentos de Seguridad de la Información*. Arbealez, Bucaramanga, Colombia: Universidad Nacional Abierta A Distancia.

Ramirez, M. (2012). *Modulo Modelos y Estándares De Seguridad Informática*. Palmira Popayán, Colombia: Universidad Nacional Abierta A Distancia.

Solarte, F. (2013). *Modulo Aspectos Éticos y Legales De Seguridad Informática.* Pasto, Colombia: Universidad Nacional Abierta A Distancia.

Suarez, L. (2013). *Modulo Sistema de Gestión de la Seguridad de la Información SGSI.* Bogotá, Colombia: Universidad Nacional Abierta A Distancia.

CIBERGRAFÍA

Ressio N. (2009) *9 pasos para implementar la seguridad informática en su empresa* Recuperado el 15 abril de 2014 de http://www.elmundodelastics.net/2009/07/9-pasospara-implementar-la-seguridad.html#.U-QXA-N5NsM.

Mundofranquicia, (2010). *La importancia de la seguridad informática en las empresas*. Recuperado el 16 de abril de 2014 de http://www.mundofranquicia.com/reportaje.php?num=520.

Mejia N. (2013) *Seguridad Informática, protección desde el principio*. Recuperado el 29 de Abril de 2014, de http://blog.smartekh.com/seguridad-informatica-proteccion-desde-el-principio/

Colombia aprende. (2014). *Penalización según la ley colombiana*, Recuperado el 12 de agosto de 2014, de http://www.colombiaaprende.edu.co/html/docentes/1596/article-73576.html#h2_2

SEG DrayTek. (2013). *Vigor 2925 Dual-WAN Router Firewall*. Recuperado el 12 de agosto de 2014 de http://www.draytek.co.uk/products/business/vigor-2925

Informática moderna. (2014). *El servidor para redes* Recuperado el 12 de agosto de 2014. de http://www.informaticamoderna.com/Servidor.htm

Hernández, E. (2009). *Seguridad y privacidad en los sistemas informáticos* Recuperado el 12 de mayo de 2014 de http://www.disca.upv.es/enheror/pdf/ACTASeguridad.PDF.

NETGEAR, (2010). *Los 8 Factores que pueden afectar a su Seguridad Informática Corporativa en las próximas dos horas*. Recuperado el 12 de mayo de 2014 de http://www.netgear.es/images/8-cosas-que-pueden-afectar-ProSecure72-41544.pdf

ESET, LLC. (2012) *Latinoamérica: el 50% de las empresas sufrió ataques de malware durante 2012*. Recuperado el 17 de junio de 2014, http://www.elinformante.cr/content/50-de-las-empresas-de-latinoam%C3%A9rica-sufri%C3%B3-ataques-de-malware-en-2012.

Disemeq Ltda. (2011) *Nosotros*. Recuperado el 11 de Agosto de 2014, de http://www.disemeqltda.com/nosotros.php

Cuerpo del proyecto

ANEXOS

- Manual de seguridad informática de DISEMEQ (se adjunta en formato PDF)
- Pantallazos del software paker Tracer con la red de la infraestructura actual y como debería quedar la red bien segmentada.

Anexo 1. Distribución de la distribución de Red actual en DISEMEQ sin seguridad

Distribución de la red actual piso 1

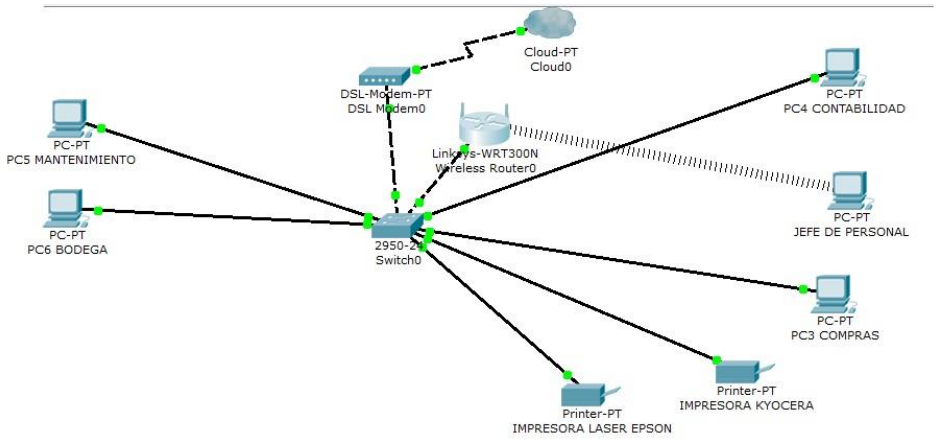


Ilustración 23. **Disemeq Ltda, *Red actual en Disemeq Ltda Piso 1* Recuperado el 15 de julio de 2014**

Cuerpo del proyecto

Distribución de la red actual piso 2

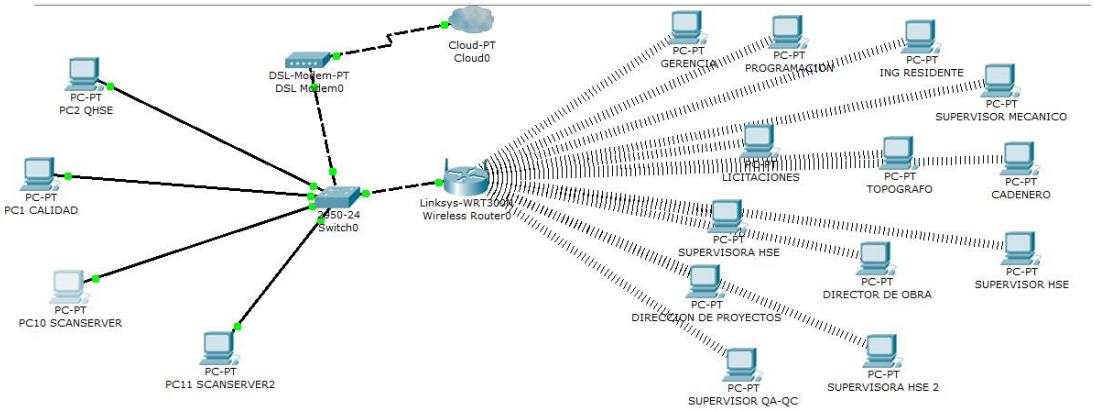


Ilustración 24. Disemeq Ltda, *Red actual en Disemeq Ltda Piso 2* Recuperado el 15 de julio de 2014

Anexo 1. Red segmentada como debe implementarse en Disemeq Ltda.

Distribución de la red a implementarse Piso 1

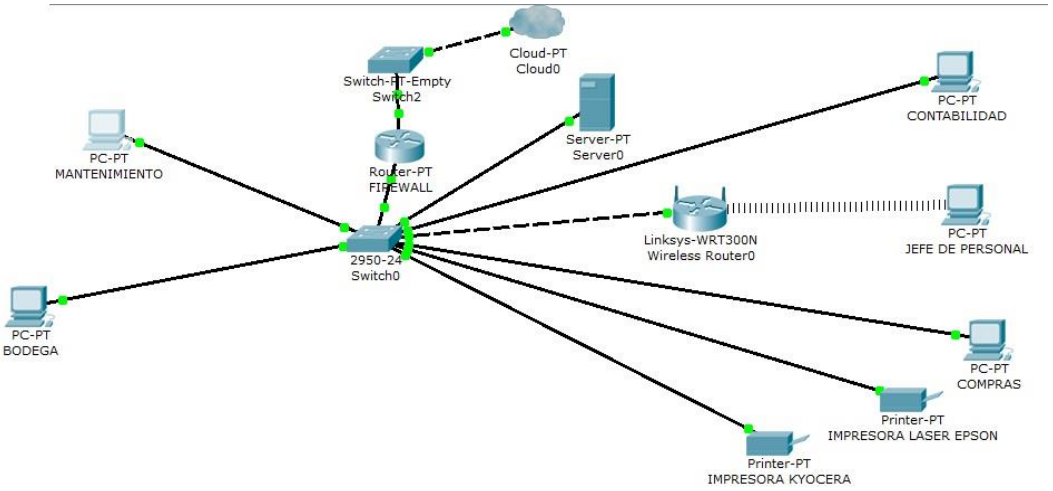


Ilustración 25. Disemeq Ltda, *Distribución de la red a implementarse Piso 1* Recuperado el 15 de julio de 2014

Cuerpo del proyecto

Distribución de la red a implementarse Piso 2

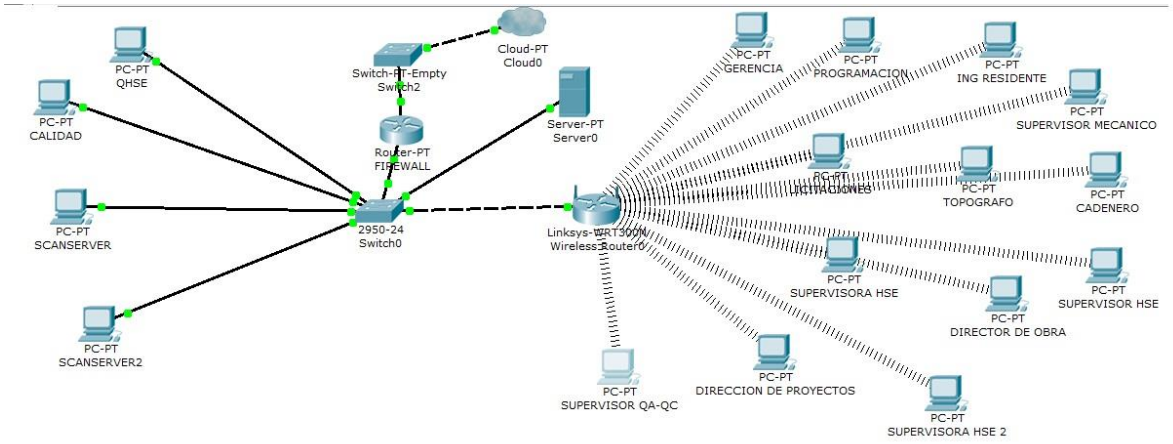
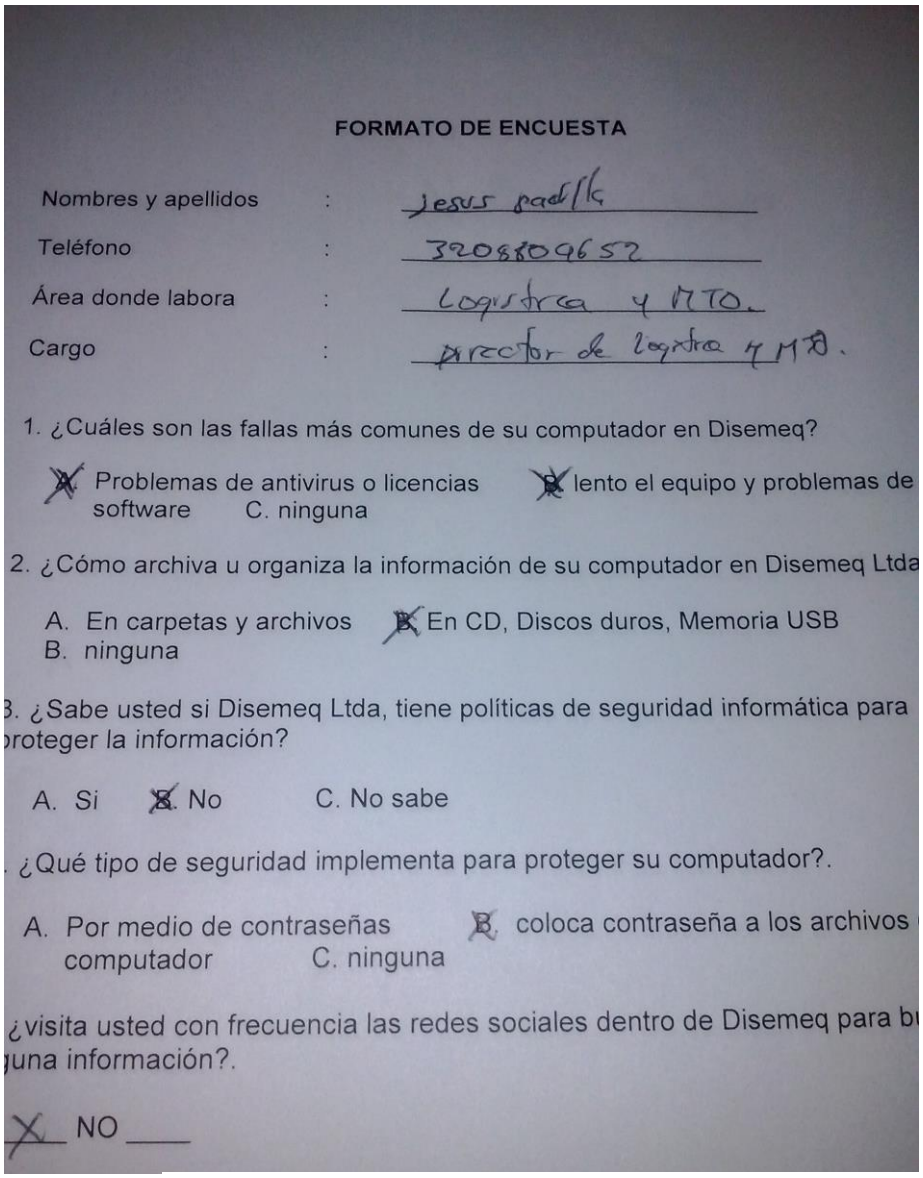


Ilustración 26. Disemeq Ltda, *Distribución de la red a implementarse Piso 2* Recuperado el 15 de julio de 2014

Cuerpo del proyecto

- ENCUESTAS REALIZADAS EN DISEMEQ

Anexo 3.



FORMATO DE ENCUESTA

Nombres y apellidos : Jesus padilla

Teléfono : 3208809652

Área donde labora : Logistica y MTO.

Cargo : Director de logistica y MTO.

1. ¿Cuáles son las fallas más comunes de su computador en Disemeq?

X Problemas de antivirus o licencias software C. ninguna X lento el equipo y problemas de

2. ¿Cómo archiva u organiza la información de su computador en Disemeq Ltda

A. En carpetas y archivos X En CD, Discos duros, Memoria USB
B. ninguna

3. ¿Sabe usted si Disemeq Ltda, tiene políticas de seguridad informática para proteger la información?

A. Si X No C. No sabe

. ¿Qué tipo de seguridad implementa para proteger su computador?.

A. Por medio de contraseñas X coloca contraseña a los archivos computador C. ninguna

¿visita usted con frecuencia las redes sociales dentro de Disemeq para b una información?.

X NO ____

Ilustración 27. Uscategui J. Formato de encuesta Realizada Recuperado el 15 de julio de 2014

Anexo 7.
Manual de seguridad Informática de DISEMEQ se adjunta en archivo PDF con 21 hojas de contenido.

Cuerpo del proyecto

Anexo 8. Carta de aceptación del Proyecto de la empresa Disemeq Ltda.

SEGURIDAD EN SU PROYECTO
CUMPLIMIENTO EN INGENIERÍA

DISEMEQ (LTDA. Cr 24 33-60, El Yopal, Casanare
WWW.DISEMEQLTDA.COM,
Fijo: ☎(57)_8 8357411, Movil (57) 315 865 8529

CARTA DE ACEPTACIÓN PROPUESTA

PROPUESTA DEL ESTADO Y NIVEL DE SEGURIDAD DE LA INFORMACIÓN VIGENTE EN LA EMPRESA DISEMEQ LTDA DEL DEPARTAMENTO DE CASANARE.

DISEMEQ LTDA

Empresa que tiene como objeto social la prestación de servicios de ingeniería, enfocada en la construcción, montaje mecánico en el sector de los hidrocarburos y mantenimiento de equipos necesarios para la ejecución de proyectos petroleros, electromecánicos, civiles y afines.

Presente.

Por medio de la presente me permito comunicar a usted que he aceptado su propuesta la cual servirá para su Tesis de grado cuyo título es "ESPECIALISTA DE SEGURIDAD INFORMATICA" en la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD", del Ingeniero JUAN ANDRES USCATEGUI NIÑO identificado con cedula de ciudadanía No. 4.104.861 de Chita Boyacá.

Atentamente

Julian Fernando Acelas G.
Jefe de recursos y gestión social.
recursos@disemeqltda.com
311-8527795
Yopal 20 de mayo de 2014.

Ilustración 28. Uscategui J. ***Carta de aceptación del Proyecto de la empresa Disemeq Ltda*** **Recuperado el 15 de julio de 2014**

Anexos

Anexo 9: MANUAL DE POLITICAS DE SEGURIDAD

MANUAL DE POLÍTICAS

DE SEGURIDAD INFORMÁTICA

EN DISEMEQ LTDA.

INDICADORES DE REVISIÓN:
1: EDICIÓN DEL DOCUMENTO, DOCUMENTO ORIGINAL.

DIRIGIDO A:

EL PRESENTE MANUAL ESTÁ DIRIGIDO A TODO EL PERSONAL DEL DISEMEQ LTDA.

CREADO POR:
ING. JUAN ANDRÉS USCATEGUI NIÑO
15 JUNIO DE 2014

Anexos

TABLA DE CONTENIDO

Anexos

Anexos

JUSTIFICACIÓN

La seguridad informática, en las empresas ha sido una de las pocas cosas que se ha venido implementando en Colombia, a lo que se refiere a una infraestructura de información, es un concepto relacionado con los componentes del sistema, las aplicaciones utilizadas en la organización y el manejo que se le dé, por parte de los usuarios, por esta razón, es un paso primordial establecer normas y estándares que permitan obtener una base de manejo seguro en lo relacionado con la infraestructura de comunicación en Disemeq Ltda.

Este manual busca resumir a los usuarios de la organización el ¿por qué?, el ¿qué? y el ¿cómo? proteger la información que fluye a través del sistema de comunicación, agrupando todas las normas y políticas relacionadas con este fin, tomándose en cuenta todos los niveles de seguridad considerados en recomendaciones internacionales.

Enfocar, dar las bases, normas de uso y seguridad informáticas dentro de Disemeq Ltda, respecto a la manipulación, uso de Software y equipos de cómputo donde nos permitirá optimizar los procesos informáticos y elevará el nivel de seguridad, y prevenir nuestra posibles falencias dentro de la organización.

Anexos

OBJETIVOS

OBJETIVO GENERAL

Realizar un manual de políticas de seguridad informática para el conocimiento y la puesta en práctica entre todo el personal de Disemeq Ltda, para evitar ataques en los computadores y la seguridad informática dentro de la organización.

OBJETIVOS ESPECÍFICOS

Elaborar un manual de políticas de seguridad informática para el personal de Disemeq Ltda, adaptado a las necesidades y adaptado a la información que se maneja en la organización.
Proporcionar un lenguaje entendible a los usuarios sobre las políticas y estándares de seguridad para la fácil aplicación en el diario vivir por parte del personal de Disemeq Ltda.
Divulgar el manual por medio de una capacitación bien fundamentada con prácticas comprensibles y de fácil entendimiento para los usuarios de Disemeq Ltda.

Anexos

ALCANCE

El presente manual describe todas las normas, políticas, estándares que se aplicarán de manera obligatoria de parte del personal de Disemeq Ltda, respecto a seguridad informática para precautelar un correcto uso de equipos de cómputo y aplicaciones tecnológicas. Los límites del alcance de este manual es que vamos a procurar enfocar a los requisitos mínimos para implementar seguridad informática en la empresa Disemeq Ltda, con los equipos que tenemos a cargo.

El manual incluye cinco capítulos, a saber:
- SEGURIDAD PERSONAL
- SEGURIDAD FÍSICA Y AMBIENTAL
- SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO
- CONTROL DE ACCESO LÓGICO
- CUMPLIMIENTO

SANCIONES DE INCUMPLIMIENTO

Las sanciones a aplicarse al personal que incumpla las normas descritas en este manual ira desde llamados de atención hasta incluso el despido o la sanción por parte de Disemeq Ltda.

INSTRUCCIONES DE INTERPRETACIÓN

El presente manual ha sido desarrollado de manera esquematizada y sencilla, con lenguaje claro para que pueda interpretarse por cualquier usuario de Disemeq Ltda, cualquiera sea su cargo e independientemente de su nivel de conocimientos informáticos.

POLÍTICAS Y NORMAS DE SEGURIDAD

Las políticas de seguridad informática, establecen la visión y actitud general a establecerse dentro del personal de la organización con respecto a los recursos y servicios tecnológicos que se utilizan. Las políticas generan a su vez las normas y estándares a aplicarse dentro de la organización para su cumplimiento; en otras palabras las políticas establecen que se entiende por seguridad dentro de una determinada organización.
Las normas son el conjunto de estándares, recomendaciones y controles que buscan cumplir los objetivos establecidos por las políticas de seguridad, las políticas establecen la concepción de seguridad dentro de la organización, las normas estableces las acciones relacionadas con ese concepto.

Anexos

POLÍTICAS Y NORMAS DE SEGURIDAD PERSONAL

POLÍTICA
Todo empleado de DISEMEQ LTDA, por trabajar en esta organización debido a sus funciones donde debe manipular, utilizar, manejar, información, equipos y servicios tecnológicos de la infraestructura de red, independientemente de su jerarquía dentro de la organización, debe firmar un convenio en el que acepte: condiciones de confidencialidad, buen manejo de información digital, buena utilización del manejo de la red, de acuerdo a sus funciones, así como manejo a las normas y políticas implementadas en este manual.

OBLIGACIONES DE LOS USUARIOS

Es responsabilidad de los usuarios de equipos y servicios tecnológicos de la empresa cumplir las políticas y normas del Manual de Políticas de Seguridad Informática para Disemeq Ltda.

ENTRENAMIENTO Y CAPACITACIÓN

Parte de los objetivos del manual es presentarse de fácil entendimiento para todo el personal cualquiera sea el nivel de conocimiento de tecnología e informática que tenga el usuario, sin embargo todos los usuarios de Disemeq Ltda, de acceso reciente debe contar con la inducción referente al Manual de Políticas de Seguridad Informática; esta tarea deberá desarrollarse por el Jefe de personal, dentro de los puntos principales de la inducción se tratará a modo general las obligaciones del usuario así como las sanciones relacionadas en caso de incumplimiento.

SANCIONES

En caso de que el Jefe de personal o jefe de sistemas, identifique el incumplimiento de las normas y políticas descritas en el presente manual, deberá emitir el reporte o informe correspondiente dirigido a parte Administrativa para que se ejecuten las medidas correspondientes. Se consideran violaciones graves el robo y daño de equipos voluntario; robo de información propia de Disemeq, además el uso de la infraestructura de comunicación de Disemeq Ltda, para hackeo o envío de correos tipo spam.

Anexos

POLÍTICAS Y NORMAS DE SEGURIDAD FÍSICA Y AMBIENTAL

POLÍTICA

Los mecanismos de control de acceso físico, deben asegurar que las áreas restringidas de Disemeq Ltda, den acceso solamente a personas autorizadas para salvaguardar la seguridad de equipos e información, dentro de estas áreas restringidas se consideran en especialmente la oficina de Gerencia y el Centro de computo. Para las estaciones de trabajo abiertas se consideran mecanismos de seguridad lógica que limiten el acceso a los equipos computacionales y la información almacenada en los mismos.

Manejo de la Información

Todos los usuarios deberán reportar de forma inmediata los riesgos reales o potenciales que presente el área física en que desempeñan sus funciones para los equipos de cómputo o de comunicación de los que hacen uso, como por ejemplo fugas de agua, incendio, etc.
Todos los medios de almacenamiento de información de tipo extraíble (diskettes, CD, DVD o memorias tipo USB) discos duros externos, en función de las tareas del usuario son responsabilidad del mismo, junto con la información contenida en los mismos, aun cuando no se utilicen.
La información almacenada en los ordenadores asignados a los funcionarios de Disemeq Ltda, son responsabilidad de los mismos, el evitar fugas o pérdidas de información dentro de los equipos es obligación del usuario.

CONTROL DE INGRESO DE EQUIPOS

Cualquier persona que acceda a las instalaciones de Disemeq Ltda, deberá registrar al momento de su ingreso: equipos de cómputo, equipos de comunicaciones, (excepto por teléfonos móviles o celulares) y herramientas que no sean propiedad de Disemeq Ltda, de manera que se mantenga control sobre el tráfico de los equipos computacionales y de computación que entran y salen de la empresa.
Las computadoras personales o portátiles asignadas o cualquier otro activo de comunicación e información podrán salir de las instalaciones de la empresa previa autorización almacén.

SEGURIDAD DEL CENTRO DE CÓMPUTO

Anexos

El centro de cómputo se considera área restringida dentro de Disemeq Ltda, sólo el personal autorizado por la administración o por el jefe de sistemas de la empresa, tiene acceso al mismo.

TRASLADO, PROTECCIÓN Y UBICACIÓN DE EQUIPOS

La reubicación o movimiento de equipos de computación y comunicación, la instalación y desinstalación de dispositivos, el retiro de sellos tanto de garantía como de licenciamiento de sistema operativo o de programas de herramientas ofimáticas son atributos de los profesionales del personal de Sistemas, este tipo de tareas se realizarán previa autorización de la administración y con apoyo de la misma.
Todo usuario es responsable de los equipos tecnológicos computacionales y de comunicación asignados en la ubicación autorizada por la parte administrativa, y el uso de los equipos será de uso exclusivo de las funciones de Disemeq Ltda.
En caso de necesitarlo, es responsabilidad del usuario solicitar capacitación necesaria para el manejo de herramientas informáticas relacionadas con su labor de forma que se reduzca el riesgo de daño o malfuncionamiento de los equipos y herramientas por mal uso o desconocimiento, optimizando al mismo tiempo el uso de las herramientas informáticas.
Toda la información obtenida y desarrollada en base a las funciones de los usuarios se guardará en la carpeta Mis Documentos, de manera que los datos puedan identificarse de manera rápida y en una sola ubicación lógica para facilitar el proceso de recuperación o respaldo de archivos.
La ingesta de alimentos y/o bebidas mientras se operan los equipos de computación y comunicación está prohibida.
La colocación de cualquier objeto sobre los equipos computacionales o la ubicación de obstáculos o cosas que obstruyan los orificios de ventilación (ubicados en la fuente y parte lateral de los CPU y monitores de los computadores) están prohibidas.
La estación de trabajo debe estar limpia de polvo y libre de humedad para disminuir daños en los equipos por estos agentes.
Los cables de conexión de los equipos computacionales a la red eléctrica, a la red de datos y el cable de conexión telefónica deben protegerse, el usuario cuidará que estos cables no sean pisados, aplastados o pinchados por personas u objetos.
Cuando se requiera cambiar la ubicación de varios equipos de cómputo (reestructuración, remodelación, cambio de lugar de unidades, etc.) Se deberá notificar a la parte Administrativa este particular con un mínimo de 48 horas de anticipación para prever las medidas a aplicarse para realizar el cambio de la manera más rápida y eficaz, todos estos movimientos y reubicaciones deben estar autorizados por la Dirección Administrativa.
Está prohibido que los usuarios abran o desarmen los equipos de computación y de comunicación asignados por Disemeq Ltda.

MANTENIMIENTO DE EQUIPOS

Anexos

Los servicios de mantenimiento y reparación se llevarán a cabo solamente por profesional encargado y previamente autorizado por la dirección administrativa es responsabilidad del usuario solicitar información e identificación de la persona o personas designadas antes de permitir el acceso al equipo asignado.

En caso de ser necesario el traslado del equipo para diagnóstico y reparación, los usuarios deberán hacer respaldos de la información que consideren crítica o relevante para sus funciones; de esta manera se asegura que la pérdida involuntaria de información que podría suceder como efecto de la reparación pueda subsanarse.

PERIFÉRICOS Y DISPOSITIVOS ESPECIALES

Los usuarios cuyos equipos computacionales están equipados con grabadores para CD, DVD o ambos utilizarán estos dispositivos exclusivamente para archivos de respaldo de documentos originales y copias de software autorizadas por Disemeq Ltda. Y deben realizar una copia de seguridad de la toda la información que manejen de la empresa mínimo una (1) vez al mes, o cuando vean que puede haber algún tipo de riesgo de pérdida de información.
El uso indebido de estos dispositivos para copias no autorizadas por el autor ("piratas") de cualquier programa de ordenador o software es responsabilidad del usuario bajo cuyo resguardo esté el equipo computacional.

DAÑO DEL EQUIPO

El daño por negligencia, maltrato o descuido del usuario en los equipos de computación y comunicación asignados será cubierto por el responsable previa verificación de la descompostura por parte de la Dirección de Administrativa; en función del daño se podrá solicitar el valor de la reparación o reposición del equipo o dispositivo.

Anexos

POLÍTICAS Y NORMAS DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

POLÍTICA

Los funcionarios de Disemeq Ltda, que utilizan equipos de computación y comunicación deben ocupar mecanismos tecnológicos para la protección y privacidad de la información que manejan y generan.
La protección de la información también compete a la prevención de código maliciosos al computador asignado, ya sea este virus, gusano, caballo de troya u otros.

USO DE MEDIOS DE ALMACENAMIENTO

No se admite el uso de archivos compartidos entre los equipos asignados, el envío y recepción de documentos internos se hará vía correo electrónico para que quede constancia del envío y de las partes relacionadas; de esta manera se asegura control sobre el flujo de comunicaciones interno de la empresa.
Todas las actividades que realizan los usuarios de la infraestructura de datos y comunicaciones de Disemeq Ltda, son susceptibles de auditoría y revisión.

INSTALACIÓN DE SOFTWARE

Todos los usuarios que debido a sus actividades requieran el uso de software propietario, deberán justificar el uso del mismo y solicitar la autorización a la Dirección administrativa a través de un oficio firmado por el jefe de personal, indicando en que equipo o equipos (de existir varias licencias adquiridas) deberá instalarse el programa en cuestión y el período de tiempo estimado de uso.
La instalación de cualquier tipo de programa en computadores, servidores o cualquier otro equipo conectado a la red sin la autorización de la administración está prohibida.

IDENTIFICACIÓN DEL INCIDENTE

En el caso que un usuario sospeche o tenga conocimiento pleno sobre un incidente de seguridad informática deberá reportarlo de inmediato a la Dirección administrativa, justificando con claridad porque lo ocurrido se considera como incidente de seguridad informática.
De existir la sospecha de que información ha sido revelada, modificada, alterada o borrada sin autorización del usuario se deberá también notificar el incidente a la gerencia.

Anexos

ADMINISTRACIÓN DE LA CONFIGURACIÓN

Está prohibido el alterar la configuración del equipo asignado por cualquier motivo, el establecer redes de área local, conexiones remotas internas o externas, el intercambio de información a través del protocolo FTP o cualquier otro protocolo de transferencia de datos tampoco está permitido sin la autorización previa de la Dirección Administrativa.

SEGURIDAD PARA LA RED

El uso del equipo computacional asignado para exploración de los recursos compartidos de la infraestructura tecnológica de Disemeq Ltda, y las aplicaciones que la misma presta con el objetivo de hallar vulnerabilidades, sin autorización previa de la Dirección Administrativa se considera un ataque a la seguridad de la red.

USO DEL CORREO ELECTRÓNICO

El correo electrónico institucional es personal e intransferible, cada usuario mantiene su propia cuenta y está prohibido el utilizar cuentas asignadas a otras personas para enviar o recibir mensajes de correo. El uso de cuentas de correos en servidores externos (Hotmail, gmail, yahoo, etc) para comunicaciones institucionales está prohibido a menos que exista autorización de la Dirección Administrativa.
Tanto los mensajes enviados y recibidos así como los archivos adjuntos que salen y entran a los buzones institucionales se consideran propiedad de Disemeq Ltda.
Disemeq Ltda, se reserva el derecho al acceso y análisis de todos los mensajes y archivos adjuntos enviados a través del correo institucional, al existir sospecha de envío de información que comprometa la seguridad de la red, o cualquier otra acción no autorizada.
El usuario debe utilizar el correo electrónico exclusivamente para desempeñar las funciones que le fueron asignadas por su cargo, empleo o comisión; cualquier otro uso del correo electrónico está prohibido.
Queda prohibido suplantar, falsear o suprimir la identidad de un usuario de correo electrónico. Queda prohibido el interceptar, revelar o ayudar a interceptar o revelar a terceros las comunicaciones por correo electrónico. El empleo del correo electrónico considera el uso de lenguaje apropiado, evitando palabras ofensivas o altisonantes que afecten la honra y estima de terceros.

CONTROLES CONTRA CÓDIGO MALICIOSO

Para evitar la inducción de código malicioso dentro de los equipos computacionales, el personal hará uso sólo del software o programas de ordenador instalados y validados por la Dirección Administrativa. Los usuarios deben verificar que toda información contenida en medios de almacenamiento extraíbles como diskettes, CD, DVD o memorias USB,

Anexos

discos externos, esté libre de códigos maliciosos, esto a través del software antivirus autorizado e instalado en cada equipo computacional por la Dirección Administrativa. Debe verificarse la presencia o no de código malicioso en todos los archivos adjuntos comprimidos (en formato .zip o .rar) enviados por personal externo o interno ejecutándose el programa antivirus autorizado antes de ejecutarse la descompresión.

El usuario que genere, compile, escriba, copie, propague o ejecute programas o aplicaciones en cualquier código o lenguaje de computadora que estén diseñados para auto-replicarse, dañar o borrar datos o impedir el funcionamiento de aplicaciones y programas autorizados o componentes del equipo computacional como memorias o periféricos será sancionado por la autoridad competente como ataque contra la seguridad informática de Disemeq Ltda.

Cualquier usuario que sospeche la infección de su equipo computacional de virus, troyano o cualquier otro código malicioso deberán dejar de usar inmediatamente el equipo y anunciar el particular a la Dirección administrativa para que se tomen las acciones respectivas de re-establecimiento del equipo y eliminación del código malicioso.

Los usuarios a quienes se han asignado equipos portátiles o que estén servicio de préstamo, están en el deber de solicitar periódicamente a la dirección administrativa la actualización del software antivirus.

Los usuarios no deben cambiar o eliminar las configuraciones de las consolas de antivirus instaladas en cada equipo computacional para prevenir la propagación de código malicioso.

Los códigos maliciosos son cada vez más complejos, por lo que ningún usuario debe intentar erradicarlos por sí mismo.

USO DEL INTERNET

El acceso a Internet provisto para el personal de Disemeq Ltda, a través de equipos computacionales es exclusivo para el desarrollo de las actividades relacionadas con las necesidades del puesto y función que desempeña. Todos los accesos de Internet deben ser provistos a través de los canales previstos para el efecto, de necesitarse una conexión a Internet especial de características diferenciadas esta debe ser notificada y autorizada por la Dirección Administrativa.

Los usuarios de internet que sospechen la ocurrencia de un incidente de seguridad informática deben reportarlo inmediatamente a la Dirección de Desarrollo Tecnológico con los justificativos respectivos sobre las sospechas para la verificación del incidente.

Todo usuario de Internet en Disemeq Ltda, al aceptar el servicio está aceptando que:

- Las actividades realizadas en Internet serán sujeto de monitoreo.
- Conocen la prohibición al acceso de páginas no autorizadas.
- Conocen la prohibición de descarga de software y archivos de música o video sin la autorización de la Dirección Administrativa.
- La utilización del Internet es para el desempeño de su función y cargo y no para propósitos personales.

Anexos

- Está prohibido el acceso a redes sociales tales como Facebook, twittter, etc ya que estas páginas albergan código malicioso, virus, y malware muy dañinos para la información.

POLÍTICAS Y NORMAS DE CONTROLES DE ACCESO LÓGICO

POLÍTICA

Cada usuario se responsabilizará por el mecanismo de acceso lógico asignado, esto es su identificador de usuario y password necesarios para acceder a la información e infraestructura de comunicación de Disemeq Ltda, es responsabilidad de cada usuario la confidencialidad de los mismos.

CONTROLES DE ACCESO LÓGICO

Todos los usuarios de equipos computacionales son responsables de la confidencialidad del identificador de usuario y el password de su equipo, así como de aplicaciones especiales que requieran el mismo control de acceso lógico.
Todos los usuarios deberán autenticarse con los mecanismos de control de acceso lógico antes de tener acceso a los recursos de la Infraestructura.
Todo el personal de Disemeq debe tener una clave segura: por tener una red inalámbrica se hace necesario incrementar los niveles de seguridad que generen seguridad al momento de realizar comunicación en este tipo de red.
En la siguiente tabla se describe cuanto tardaría un hacker en enterarse de tu contraseña. Noten que no se necesitan contraseñas kilométricas para hacerlas más seguras, dado que en una contraseña de 9 caracteres, únicamente variando algunas pocas cosas (agregando una mayúscula por ejemplo), la contraseña pasa a tener una fortaleza muy importante. Teniendo en cuenta esta tabla, ¿cuán seguras son tus contraseñas?[13].

La forma correcta de crear una clave es así:

Tabla 3. Información de http://adictamente.blogspot.com/2011/06/facil-manera-de-crear-contrasenas.html

Largo	Minúsculas	Agrega Mayúscula	Números y Símbolos
6 caracteres	10 minutos	10 horas	18 días
7 caracteres	4 horas	23 días	4 años
8 caracteres	4 días	3 años	463 años
9 caracteres	4 meses	178 años	44.530 años

[13] Tomado de http://adictamente.blogspot.com/2011/06/facil-manera-de-crear-contrasenas.html

Anexos

Ejemplo de contraseña segura: li23LO56q
No está permitido a los usuarios el proporcionar información a personal externo sobre los mecanismos de control de acceso a los recursos e infraestructura tecnológica, salvo el caso de autorización expresa del generador de la información y la Dirección administrativa.
El identificador de usuario dentro de la red es único y personalizado, no está permitido el uso del mismo identificador de usuario por varios miembros del personal.
El usuario es responsable de todas las actividades realizadas con su identificador de usuario, por tanto no debe divulgar ni permitir que terceros utilicen su identificador, al igual que está prohibido usar el identificador de usuario de otros.

ADMINISTRACIÓN DE PRIVILEGIOS

Todo cambio en roles, funciones o cargo que requiera asignar al usuario atributos para acceso a diferentes prestaciones de la infraestructura tecnológica debe ser notificado a la Dirección administrativa o la unidad que ordena el cambio.

EQUIPO DESANTENDIDO

El usuario que deja su lugar de trabajo por cualquier razón debe dejar bloqueado su terminal o equipo computacional precautelando la seguridad de la información a través del mecanismo de control de acceso lógico.

ADMINISTRACIÓN Y USO DE PASSWORDS

Es obligación del usuario cambiar la clave por defecto asignada por la Dirección administrativa. Los passwords son individuales, está prohibido que varios usuarios compartan un password. Cuando un usuario olvide, bloquee o extravíe su password deberá solicitar a la Dirección administrativa para que se le realice la acción que le permita ingresar un nuevo password, y el momento de recibirlo deberá personalizar uno nuevo.
Está prohibido mantener ayudas escritas o impresas referentes al password en lugares donde personas no autorizadas pueden descubrirlos.
La revelación del password o contraseña a terceros responsabiliza al usuario que prestó su password de todas las acciones que se realicen con el mismo.

CONTROL DE ACCESOS REMOTOS

El uso de las extensiones telefónicas para acceso al Internet de tipo Dial-Up está prohibido, se considera excepción previa autorización. La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con la autorización y un

Anexos

mecanismo de control de acceso seguro autorizado por el dueño de la información y la Dirección administrativa.

POLÍTICAS Y NORMAS DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

POLÍTICA
Disemeq Ltda, emitirá y revisará el cumplimiento de las políticas y normas de seguridad informática que permitan realizar acciones correctivas y preventivas para el cuidado y mantenimiento de los equipos que forman parte de la infraestructura tecnológica.

DERECHOS DE PROPIEDAD INTELECTUAL

Las leyes de propiedad intelectual prohíben la reproducción de programas de ordenador o software sin autorización escrita del autor, ya sea este adquirido o desarrollado en Disemeq Ltda.

REVISIONES DE CUMPLIMIENTO

Disemeq Ltda, realizará acciones de verificación del cumplimiento de manual de políticas de seguridad informática, lo que incluye mecanismos de revisión de tendencias en el uso de recursos informáticos y la naturaleza de los archivos procesados.
El mal uso de los recursos informáticos detectado por la empresa será reportado conforme a lo indicado en la política de Seguridad de Personal en Disemeq Ltda.

VIOLACIONES DE SEGURIDAD INFORMÁTICA

Se prohíbe el uso de herramientas de hardware o software que alteren o eviten los controles de seguridad informática, a menos que exista autorización expresa de la Dirección Administrativa.
La búsqueda de orificios o fallas de seguridad informática está reservada para la Dirección Administrativa, está prohibida la realización de pruebas de este tipo para cualquier usuario no autorizado.
La propagación de código malicioso de forma intencional para probar el desempeño de la red de parte de usuarios no autorizados está prohibida totalmente.

GLOSARIO DE TÉRMINOS

Dispositivos de almacenamiento: son recursos para almacenar información tales como cd, dvd, discos duros externos, unidad USB etc.

Anexos

Claves alfanuméricas: son contraseñas creadas por el usuario compuestas por números y letras que proporcionan seguridad en el momento de acceder a una equipo o recurso.
CPU: (Unidad Central de proceso): Abreviatura utilizada para nombrar al procesador de un ordenador, que es el chip que maneja las operaciones lógicas de cada proceso, en la práctica se usa también para denominar a todo el equipamiento que contiene al procesador.
DVD: (disco digital verstátil): Unidad de almacenamiento óptica en forma de disco de alta densidad que permite manejar formatos de audio y video de alta calidad y gran capacidad de almacenamiento de datos, sustituto natural del CD ya que soporta más de 4 veces la capacidad de este.

FTP: (File Transfer Protocol, protocolo de transferencia de archivos): Protocolo que permite la transferencia de archivos en la mayoría de redes actuales, FTP es soportado por varios sistemas operativos, incluidas todas las versiones actuales del Windows.
Gusano: Se denomina gusano al tipo de código malicioso capaz de duplicarse a sí mismo, suele usar las operaciones automáticas de archivos propios del sistema operativo del computador para la copia de sí mismo; básicamente ataca la red en sí ya que la duplicación ocupa ancho de banda y enlentece los procesos.

Hackeo: En el presente documento se limita a la acción de hallar huecos de seguridad en la infraestructura de una red para acceder a la información de la misma.
MB: (Megabyte): Unidad de volumen de información digital equivale a 1024 bytes, el byte agrupa a ocho bits, un bit es la unidad fundamental del sistema digital y toma un valor de uno (1) o cero (0).

RAR: Formato de compresión, un archivo de cualquier naturaleza puede comprimirse a través de un software especializado y toma la extensión .rar.

Software: Se denomina software a todo programa, que instalado en un computador permite el acceso al usuario a la manipulación de información o uso de periféricos como impresoras, videocámaras u otros.

Spam: Publicidad no solicitada que viaja a través de cualquier red hacia buzones de correo electrónico, el envío de spam en la red de Internet es uno de los mayores causantes de saturación de la red.

Troyano: Un troyano es un tipo de código malicioso capaz de ingresar a un ordenador para recabar información que permita el acceso de usuarios externos al computador local con los consiguientes problemas de seguridad informática.

USB: (Universal Serial Bus, Bus serial universal): Es un tipo de puerto formado por 4 terminales para recepción, transmisión, y energización del equipo; los puertos USB se encuentran presentes en todas las computadoras actuales y permiten la conexión de unidades de almacenamiento portátiles, cámaras, teléfonos, módems inalámbricos y todo tipo de periféricos.

Anexos

Virus: Un virus es un tipo de código malicioso capaz de destruir o alterar información del computador que lo aloja.
ZIP: Formato de compresión de datos, un archivo de cualquier tipo como imágenes, programas, etc. se puede comprimir a través de un software y toma la extensión .zip.

RECOMENDACIONES PARA EL GERENTE DE DISEMEQ LTDA.

- Todo el personal de Disemeq ltda, se debe capacitar para darle a conocer este manual de políticas de seguridad y ponerlo en práctica dentro de la organización. Ya que si no lo hacemos estamos de una u otra forma dando vulnerabilidad para que nuestra información sea atacada por extraños que quieran hacer daño a nuestra empresa.

- Todo el personal de Disemeq ltda, debe firmar dentro de su contrato laboral, una clausula donde se comprometa dentro de sus funciones a unas condiciones de confidencialidad, buen manejo de información digital, buena utilización del manejo de la red, de acuerdo a sus funciones, así como manejo a las normas y políticas implementadas en este manual.

- Cada empleado de Disemeq ltda, es responsable de la buena administración de su información, por tal razón está obligado a realizar copias de seguridad de la información que maneje dentro de su cargo y debe darle una copia mensual al jefe de personal para evitar pérdidas de información ocasionado por una falla mecánica o eléctrica. Es importante aclarar que para prevenir la perdida de datos es mejor mantener múltiples respaldos de la información, como en discos duros, CD, DVD, memorias etc.

- Cada empleado debe crear contraseñas confiables para su computador, correo electrónico, bases de datos y acceso de cualquier tipo a un sistema según como lo indica las políticas de seguridad de este manual.